



Jay E. Gruber
General Attorney

Room 420
99 Bedford Street
Boston, MA 02111
617 574-3149
FAX (281) 664-9929
iegruber@att.com

June 15, 2006

BY OVERNIGHT MAIL

Thomas F. Ahern, Administrator
Division of Public Utilities and Carriers
89 Jefferson Boulevard
Warwick, RI 02888

Re: Complaint and request for investigation of Verizon and AT&T

Dear Mr. Ahern:

Pursuant to your letter to Mr. William [Leahy], dated May 25, 2006, this letter is to respond on behalf of AT&T to the informal complaint of the Rhode Island Affiliate, American Civil Liberties Union ("RI-ACLU") filed on May 24, 2006 ("Complaint") with the Rhode Island Division of Public Utilities and Carriers ("Division"). The Complaint makes certain allegations regarding Verizon and AT&T's putative sharing of telephone records with the National Security Agency ("NSA") and asks the Division to investigate and, if appropriate, take remedial action. As described in more detail below, the Division's examination of these issues is neither appropriate nor even possible in light of the national security concerns that have already been raised by the United States and, as the Federal Communications Commission ("FCC") has already indicated, in view of the federal government's state secrets privilege. For this reason and for all the reasons set forth below, we urge the Division to decline to initiate any proceedings relating to alleged NSA surveillance activities.

The litigation against AT&T and other carriers arises primarily from press reports concerning certain alleged activities of the NSA. On December 19, 2005, in response to a report in the New York Times, President Bush acknowledged the existence of a counterterrorism program involving the interception of international telephone calls made or received by suspected al Qaeda agents.¹ The United States Department of Justice subsequently published a

¹ See Press Conference of President Bush (Dec. 19, 2005), available at <http://www.whitehouse.gov/news/releases/2005/12/20051219-2.html>; Press Conference of Attorney General Alberto Gonzales and General Michael Hayden, Principal Deputy Director for

written explanation of the legal authority for the program acknowledged by the President and defended by the Attorney General.² On May 11, 2006, USA Today published a story suggesting that the NSA's intelligence activities may also have included some form of access to domestic call records databases.³ The Administration has neither confirmed nor denied these more recent reports.

AT&T has consistently declined either to confirm or deny any participation in these programs. As a matter of policy, AT&T declines comment on matters related to national security. AT&T has, however, affirmed that any cooperation it affords the law enforcement or intelligence communities occurs strictly in accordance with law.

On January 31, 2006, following publication of the original New York Times story, a nationwide class action lawsuit was filed against the AT&T Defendants in the United States District Court for the Northern District of California. *See Hepting v. AT&T*, No. C-06-0672-VRW (N.D. Cal.). That lawsuit alleges that one or more of the AT&T Defendants cooperated with various NSA national security surveillance activities and, in so doing, violated the First and Fourth Amendments of the U.S. Constitution and various provisions of the Foreign Intelligence Surveillance Act ("FISA"), the Electronic Communications Privacy Act ("ECPA"), the Communications Act of 1934, and California state law. Following publication of the USA Today story on May 11, a series of additional class actions were filed, in both state and federal courts, making similar allegations. To date, more than twenty such actions have been filed against the AT&T Defendants and other carriers in courts around the country. On May 24, 2006, a petition was filed with the Judicial Panel on Multidistrict Litigation seeking to consolidate these actions before a single federal district court for pretrial proceedings.⁴ Among other reasons, the MDL petition cites the unique national security concerns involved in these cases and the possible need to share highly classified information with federal judges as justifications for consolidating all of the pending actions in a single federal judicial district for joint consideration.

To date, the only lawsuit that has proceeded past the filing of the complaint is the original *Hepting* matter in the Northern District of California. In *Hepting*, the AT&T Defendants responded by filing a motion to dismiss the suit, on various grounds including that the maintenance of any claim or cause of action is prohibited by a number of well-established

National Intelligence (Dec. 19, 2005), available at <http://www.whitehouse.gov/news/releases/2005/12/20051219-1.html>.

² See United States Department of Justice Memorandum, *Legal Authorities Supporting the Activities of the National Security Agency Described by the President*, (January 19, 2006) (Attachment A).

³ Leslie Cauley, *NSA Has Massive Database of Americans' Phone Calls*, USA Today, May 11, 2006, at A1.

⁴ See Defendants Verizon Communications Inc., Verizon Global Networks Inc., and Verizon Northwest Inc.'s Motion for Transfer and Coordination Pursuant to 28 U.S.C. § 1407, *In re National Security Agency Litigation*, Judicial Panel on Multidistrict Litigation (May 24, 2006) (Attachment B).

statutory and common-law immunities. Telecommunications carriers enjoy these broad immunities when acting at the direction and with the assurances of the government to provide facilities, assistance or information to the government in connection with national security-related surveillance and intelligence activities.⁵

Shortly after the AT&T motions were filed, the United States intervened in the *Hepting* case and sought dismissal of the action in its entirety “because adjudication of Plaintiffs’ claims risks or requires the disclosure of protected state secrets and would thereby risk or cause exceptionally grave harm to the national security of the United States.”⁶ The state secrets privilege that the United States has invoked is a well-established, constitutionally-based privilege belonging exclusively to the federal government that protects any information whose disclosure would result in “impairment of the nation’s defense capabilities” or “disclosure of intelligence-gathering methods or capabilities.” *Ellsberg v. Mitchell*, 709 F.2d 51, 57 (D.C. Cir. 1983). The invocation of state secrets must be made formally through an affidavit by “the head of the department which has control over the matter, after actual personal consideration by the officer.” *United States v. Reynolds*, 345 U.S. 1, 7-8 (1953). As the United States noted in its motion, when the entire subject matter of a controversy is a state secret, then the matter must be dismissed outright, and no balancing of competing considerations is allowed or sufficient to override the privilege. *See, e.g., Kasza v. Browner*, 133 F.3d 1159, 1166 (9th Cir. 1998).

In seeking dismissal of the *Hepting* lawsuit, the United States indicated that “no aspect of this case can be litigated without disclosing state secrets.”⁷ In particular, the United States has asserted the state secrets privilege with respect to “the existence, scope, and potential targets of alleged intelligence activities, as well AT&T’s alleged involvement in such activities.”⁸ In support of this assertion, the United States submitted a classified declaration from Director of National Intelligence John D. Negroponte, in which Ambassador Negroponte, “who bears statutory authority as head of the United States Intelligence Community to protect intelligence sources and methods, . . . formally asserted the state secrets privilege after personal consideration of the matter.”⁹ Supported by a classified declaration from Director of the National Security Agency General Keith B. Alexander, Ambassador Negroponte “demonstrated the exceptional

⁵ *See* Motion of Defendant AT&T Corp. to Dismiss Plaintiffs’ Amended Complaint; Supporting Memorandum, *Hepting, et al. v. AT&T Corp., et al.*, Case No. C 06-0672-VRW (N.D. Cal.) (April 28, 2006) (Attachment C).

⁶ Notice of Motion and Motion to Dismiss or, in the Alternative, for Summary Judgment by the United States of America, at 29, *Hepting, et al. v. AT&T Corp., et al.*, Case No. C 06-0672-VRW (N.D. Cal.) (May 12, 2006) (Attachment D).

⁷ United States’ Response to Plaintiffs’ Memorandum of Points and Authorities in Response to Court’s May 17, 2006 Minute Order, *Hepting, et al. v. AT&T Corp., et al.*, Case No. C 06-0672-VRW, at 1 (N.D. Cal.) (May 24, 2006) (Attachment E).

⁸ Notice of Motion and Motion to Dismiss or, in the Alternative, for Summary Judgment by the United States of America, *supra* note 6, at 16.

⁹ *Id.* at 12. The public version of Ambassador Negroponte’s declaration is Attachment F.

harm that would be caused to U.S. national security interests by disclosure” of information pertaining to the alleged surveillance activities and any information tending to confirm or deny AT&T’s claimed participation in those activities.¹⁰ By separate filings on May 24, 2006, both the United States and AT&T urged the district court to review the classified versions of the United States’ briefs and declarations prior to oral arguments on the motions to dismiss, which are now scheduled for June 23, 2006.¹¹ In a June 6 Order, the district court agreed that the litigation cannot proceed and that no discovery can occur until the court conducts an *ex parte* and *in camera* review of the classified memorandum and classified declarations of Ambassador Negroponte and General Alexander and determines whether the states secrets privileges has been properly asserted. The Court held that the potential for “exceptionally grave damage to the national security of the United States” precluded any disclosure of information about the alleged surveillance until the threshold states secret issue has been resolved.¹²

In parallel with this litigation, certain members of Congress urged the Federal Communications Commission to investigate the reports that AT&T and other telecommunications carriers had shared call record data with the NSA or otherwise violated the privacy protections in the Communications Act. After reviewing the matter, including the submissions of the United States in *Hepting*, the FCC concluded that “it would not be possible for us to investigate the activities addressed in your letter without examining highly sensitive classified information.”¹³ Because “[t]he Commission has no power to order the production of classified information,” and because section 6 of the National Security Act of 1959 independently prohibits disclosure of information relating to NSA activities, the Commission informed the Congress that it lacked authority to compel the production of the information necessary to undertake an investigation and would not do so.¹⁴ Finally, while the Chairman of the Senate Judiciary Committee had at one time suggested that he might conduct hearings into the activities of telecommunications carriers, he has announced that no such hearings will occur now. These issues are within the jurisdiction of the House and Senate Select Committees on Intelligence, which are constituted to prevent disclosure of classified information.¹⁵

¹⁰ *Id.* at 13. The public version of General Alexander’s declaration is Attachment G.

¹¹ See United States’ Response to Plaintiffs’ Memorandum of Points and Authorities in Response to Court’s May 17, 2006 Minute Order, *supra* Note 7; Reply Memorandum of Defendant AT&T Corp. in Response to Court’s May 17, 2006 Minute Order, *Hepting, et al. v. AT&T Corp., et al.*, Case No. C 06-0672-VRW, N.D.Ca (May 24, 2006) (Attachment H).

¹² June 6 Order, *Hepting, et al. v. AT&T Corp., et al.*, Case No. C 06-0672-VRW, N.D.Ca (June 6, 2006) (Attachment I).

¹³ Letter from Kevin J. Martin, Chairman Federal Communications Commission to the Honorable Edward J. Markey, at 1 (May 22, 2006) (Attachment J).

¹⁴ *Id.* at 2.

¹⁵ CNN, *Specter won’t ask telcos to testify on taps*, CNN.Com, June 6, 2006, available at http://money.cnn.com/2006/06/06/news/companies/telco_nsa.

In light of the foregoing, we respectfully submit that the Division should decline to initiate any proceedings relating to alleged NSA surveillance activities. The alleged cooperation of telecommunications carriers with the United States Intelligence Community is currently under review in the federal courts and in the United States Congress. The Federal Communications Commission has already recognized that administrative review by telecommunications regulators is infeasible and inappropriate. Moreover, any such investigation would be duplicative and unnecessary and would increase the risk of inadvertent disclosure of highly classified information.

In any event, given the state secrets and classified information at the core of these alleged intelligence activities, the Division could not adduce any evidence on which to base any informed conclusions. The United States' state secrets assertion in *Hepting* covers all details of the alleged NSA activities at issue, including the identities of any carriers participating in it and their roles and responsibilities, if any. All carriers are disabled from responding to requests for information on this subject. The state secrets privilege cannot be waived by a private party, *see United States v. Reynolds*, 345 U.S. 1, 7 (1953), and AT&T could therefore neither confirm nor deny any participation in any alleged intelligence activities of the NSA. In addition, it is a federal felony for any person to divulge classified information "concerning the communication intelligence activities of the United States" to any person not authorized to receive such information. 18 U.S.C. § 798. There are also independent statutory prohibitions on divulging information or records pertaining to surveillance activities undertaken pursuant to FISA or ECPA, as well as the activities of the NSA. *See* 50 U.S.C. §§ 1805(c)(2)(B), (C); 18 U.S.C. § 2511(2)(a)(ii)(B); 50 U.S.C. § 402 note; *Founding Church of Scientology v. NSA*, 610 F.2d 824, 828 (D.C. Cir. 1979) (50 U.S.C. § 402 note reflects congressional judgment that information pertaining to activities of NSA "ought to be safe from forced exposure"). Collectively, these federal enactments preclude the possibility that state officials can or should undertake responsibility for investigating a telecommunications carrier's role, if any, in the NSA's intelligence activities.

These points are dramatically underscored by recent events that occurred in New Jersey. On May 17, 2006, the New Jersey Attorney General had served AT&T and other carriers with a subpoena that sought documents and other information relating to AT&T's alleged activities under the NSA program. The return date for this subpoena was June 15, 2006. On June 14, 2006, the United States filed suit in the United States District Court for the District of New Jersey against the New Jersey Attorney General, AT&T, and other carriers, seeking a declaratory judgment that federal law prohibits New Jersey from enforcing the Subpoenas and prohibits AT&T from providing the requested information to state officials.¹⁶ In this lawsuit, the United States maintains that state attempts to force carriers to disclose information about their activities, if any, under the NSA Program relate to exclusively federal functions and are preempted by a number of different provisions of federal law.

¹⁶ *See* Complaint, *United States of America v. Zulima V. Farber, et al.*, Civil Action No. _____, Prayer for Relief ¶ 1, (D.N.J.) (June 14, 2006) (Attachment K).

The United States explained these allegations in greater detail in a letter that was simultaneously sent to the New Jersey Attorney General.¹⁷ There, the United States stated that state subpoenas seeking information relating to the NSA Program "intrude upon a field that is reserved exclusively to the Federal Government and in a manner that interferes with federal prerogatives" and that "[r]esponding to the subpoenas," and even merely "disclosing whether or to what extent any responsive materials exist, would violate various specific provisions of federal statutes and Executive Orders," including provisions that carry criminal sanctions.¹⁸ The United States also explained that the subpoenas "seek the disclosure of matters with respect to which the D[irector of] N[ational] I[n]telligence] already has determined that disclosure, including confirming or denying whether or to what extent such materials exist, would improperly reveal intelligence sources and methods" in contravention of the United States' state secrets privilege.¹⁹

At the same time the United States filed this lawsuit, it sent a letter to AT&T that specifically advised that "[r]esponding to the subpoenas - including by disclosing whether or to what extent any responsive materials exist - would violate federal laws and Executive Orders."²⁰ Accordingly, AT&T is advising the New Jersey Attorney General that it cannot disclose any of the requested information regarding AT&T's activities, if any, under the NSA program, pending the final resolution of these issues in the federal judicial system. This underscores that state commission efforts to investigate the allegations against AT&T cannot proceed in view of the positions taken by the United States.

In closing, we wish to emphasize that the press reports on which the various complaints have been based provide no basis for assuming illegality on the part of any carrier. There are numerous avenues by which the cooperation of telecommunications carriers such as AT&T with federal law enforcement, investigative, or intelligence agencies is not only authorized but required, and, as noted, federal law accordingly provides absolute immunity from suit to carriers in such circumstances and a broad "good faith" defense even to actions that survive that immunity.²¹

¹⁷ Letter from Peter D. Keisler to the Honorable Zulima V. Farber, at 1, 5 (June 14, 2006) (Attachment L).

¹⁸ *Id.* at 2-3.

¹⁹ *Id.* at 5.

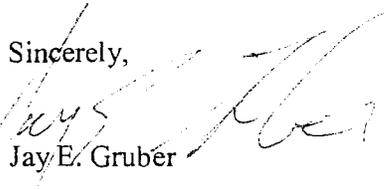
²⁰ Letter from Peter D. Keisler to Bradford A. Berenson, Esq., et al., at 1 (June 14, 2006) (Attachment M).

²¹ *See, e.g.*, 18 U.S.C. §§ 2511(2), 2511(3), 2520(d), 2702(b), 2702(c), 2707(e), 2703, 2709, 3124(d) & (e); 50 U.S.C. §§ 1805(f) & (i), 1842(f), 1843.

Mr. Thomas F. Ahern
June 15, 2006
Page 7 of 7

AT&T therefore respectfully requests that the Division take no further action in this matter.

Sincerely,



Jay E. Gruber

cc: William P. Leahy, Vice President, External Affairs – Atlantic Region, AT&T

Enclosures

EXHIBIT A



Office of the Attorney General
Washington, D.C.

January 19, 2006

The Honorable William H. Frist
Majority Leader
United States Senate
Washington, D.C. 20510

Dear Mr. Leader:

As the President recently described, in response to the attacks of September 11th, he has authorized the National Security Agency (NSA) to intercept international communications into or out of the United States of persons linked to al Qaeda or an affiliated terrorist organization. The attached paper has been prepared by the Department of Justice to provide a detailed analysis of the legal basis for those NSA activities described by the President.

As I have previously explained, these NSA activities are lawful in all respects. They represent a vital effort by the President to ensure that we have in place an early warning system to detect and prevent another catastrophic terrorist attack on America. In the ongoing armed conflict with al Qaeda and its allies, the President has the primary duty under the Constitution to protect the American people. The Constitution gives the President the full authority necessary to carry out that solemn duty, and he has made clear that he will use all authority available to him, consistent with the law, to protect the Nation. The President's authority to approve these NSA activities is confirmed and supplemented by Congress in the Authorization for Use of Military Force (AUMF), enacted on September 18, 2001. As discussed in depth in the attached paper, the President's use of his constitutional authority, as supplemented by statute in the AUMF, is consistent with the Foreign Intelligence Surveillance Act and is also fully protective of the civil liberties guaranteed by the Fourth Amendment.

It is my hope that this paper will prove helpful to your understanding of the legal authorities underlying the NSA activities described by the President.

Sincerely,

A handwritten signature in cursive script, appearing to read "A. Gonzales".

Alberto R. Gonzales
Attorney General

Enclosure

cc: The Honorable Harry Reid
Minority Leader

16a



U.S. Department of Justice

Washington, D.C. 20530

January 19, 2006

**LEGAL AUTHORITIES SUPPORTING THE ACTIVITIES OF THE
NATIONAL SECURITY AGENCY DESCRIBED BY THE PRESIDENT**

As the President has explained, since shortly after the attacks of September 11, 2001, he has authorized the National Security Agency ("NSA") to intercept international communications into and out of the United States of persons linked to al Qaeda or related terrorist organizations. The purpose of these intercepts is to establish an early warning system to detect and prevent another catastrophic terrorist attack on the United States. This paper addresses, in an unclassified form, the legal basis for the NSA activities described by the President ("NSA activities").

SUMMARY

On September 11, 2001, the al Qaeda terrorist network launched the deadliest foreign attack on American soil in history. Al Qaeda's leadership repeatedly has pledged to attack the United States again at a time of its choosing, and these terrorist organizations continue to pose a grave threat to the United States. In response to the September 11th attacks and the continuing threat, the President, with broad congressional approval, has acted to protect the Nation from another terrorist attack. In the immediate aftermath of September 11th, the President promised that "[w]e will direct every resource at our command—every means of diplomacy, every tool of intelligence, every tool of law enforcement, every financial influence, and every weapon of war—to the destruction of and to the defeat of the global terrorist network." President Bush Address to a Joint Session of Congress (Sept. 20, 2001). The NSA activities are an indispensable aspect of this defense of the Nation. By targeting the international communications into and out of the United States of persons reasonably believed to be linked to al Qaeda, these activities provide the United States with an early warning system to help avert the next attack. For the following reasons, the NSA activities are lawful and consistent with civil liberties.

The NSA activities are supported by the President's well-recognized inherent constitutional authority as Commander in Chief and sole organ for the Nation in foreign affairs to conduct warrantless surveillance of enemy forces for intelligence purposes to detect and disrupt armed attacks on the United States. The President has the chief responsibility under the Constitution to protect America from attack, and the Constitution gives the President the authority necessary to fulfill that solemn responsibility. The President has made clear that he will exercise all authority available to him, consistent with the Constitution, to protect the people of the United States.

(166)

In the specific context of the current armed conflict with al Qaeda and related terrorist organizations, Congress by statute has confirmed and supplemented the President's recognized authority under Article II of the Constitution to conduct such warrantless surveillance to prevent further catastrophic attacks on the homeland. In its first legislative response to the terrorist attacks of September 11th, Congress authorized the President to "use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks" of September 11th in order to prevent "any future acts of international terrorism against the United States." Authorization for Use of Military Force, Pub. L. No. 107-40, § 2(a), 115 Stat. 224, 224 (Sept. 18, 2001) (reported as a note to 50 U.S.C.A. § 1541) ("AUMF"). History conclusively demonstrates that warrantless communications intelligence targeted at the enemy in time of armed conflict is a traditional and fundamental incident of the use of military force authorized by the AUMF. The Supreme Court's interpretation of the AUMF in *Hamdi v. Rumsfeld*, 542 U.S. 507 (2004), confirms that Congress in the AUMF gave its express approval to the military conflict against al Qaeda and its allies and thereby to the President's use of all traditional and accepted incidents of force in this current military conflict—including warrantless electronic surveillance to intercept enemy communications both at home and abroad. This understanding of the AUMF demonstrates Congress's support for the President's authority to protect the Nation and, at the same time, adheres to Justice O'Connor's admonition that "a state of war is not a blank check for the President," *Hamdi*, 542 U.S. at 536 (plurality opinion), particularly in view of the narrow scope of the NSA activities.

The AUMF places the President at the zenith of his powers in authorizing the NSA activities. Under the tripartite framework set forth by Justice Jackson in *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 635-38 (1952) (Jackson, J., concurring), Presidential authority is analyzed to determine whether the President is acting in accordance with congressional authorization (category I), whether he acts in the absence of a grant or denial of authority by Congress (category II), or whether he uses his own authority under the Constitution to take actions incompatible with congressional measures (category III). Because of the broad authorization provided in the AUMF, the President's action here falls within category I of Justice Jackson's framework. Accordingly, the President's power in authorizing the NSA activities is at its height because he acted "pursuant to an express or implied authorization of Congress," and his power "includes all that he possesses in his own right plus all that Congress can delegate." *Id.* at 635.

The NSA activities are consistent with the preexisting statutory framework generally applicable to the interception of communications in the United States—the Foreign Intelligence Surveillance Act ("FISA"), as amended, 50 U.S.C. §§ 1801-1862 (2000 & Supp. II 2002), and relevant related provisions in chapter 119 of title 18.¹ Although FISA generally requires judicial approval of electronic surveillance, FISA also contemplates that Congress may authorize such surveillance by a statute other than FISA. See 50 U.S.C. § 1809(a) (prohibiting any person from intentionally "engag[ing] . . . in electronic surveillance under color of law except as authorized

¹ Chapter 119 of title 18, which was enacted by Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended, 18 U.S.C. §§ 2510-2521 (2000 & West Supp. 2005), is often referred to as "Title III."

by statute"). The AUMF, as construed by the Supreme Court in *Hamdi* and as confirmed by the history and tradition of armed conflict, is just such a statute. Accordingly, electronic surveillance conducted by the President pursuant to the AUMF, including the NSA activities, is fully consistent with FISA and falls within category I of Justice Jackson's framework.

Even if there were ambiguity about whether FISA, read together with the AUMF, permits the President to authorize the NSA activities, the canon of constitutional avoidance requires reading these statutes in harmony to overcome any restrictions in FISA and Title III, at least as they might otherwise apply to the congressionally authorized armed conflict with al Qaeda. Indeed, were FISA and Title III interpreted to impede the President's ability to use the traditional tool of electronic surveillance to detect and prevent future attacks by a declared enemy that has already struck at the homeland and is engaged in ongoing operations against the United States, the constitutionality of FISA, as applied to that situation, would be called into very serious doubt. In fact, if this difficult constitutional question had to be addressed, FISA would be unconstitutional as applied to this narrow context. Importantly, the FISA Court of Review itself recognized just three years ago that the President retains constitutional authority to conduct foreign surveillance apart from the FISA framework, and the President is certainly entitled, at a minimum, to rely on that judicial interpretation of the Constitution and FISA.

Finally, the NSA activities fully comply with the requirements of the Fourth Amendment. The interception of communications described by the President falls within a well-established exception to the warrant requirement and satisfies the Fourth Amendment's fundamental requirement of reasonableness. The NSA activities are thus constitutionally permissible and fully protective of civil liberties.

BACKGROUND

A. THE ATTACKS OF SEPTEMBER 11, 2001

On September 11, 2001, the al Qaeda terrorist network launched a set of coordinated attacks along the East Coast of the United States. Four commercial jetliners, each carefully selected to be fully loaded with fuel for a transcontinental flight, were hijacked by al Qaeda operatives. Two of the jetliners were targeted at the Nation's financial center in New York and were deliberately flown into the Twin Towers of the World Trade Center. The third was targeted at the headquarters of the Nation's Armed Forces, the Pentagon. The fourth was apparently headed toward Washington, D.C., when passengers struggled with the hijackers and the plane crashed in Shanksville, Pennsylvania. The intended target of this fourth jetliner was evidently the White House or the Capitol, strongly suggesting that its intended mission was to strike a decapitation blow on the Government of the United States—to kill the President, the Vice President, or Members of Congress. The attacks of September 11th resulted in approximately 3,000 deaths—the highest single-day death toll from hostile foreign attacks in the Nation's history. These attacks shut down air travel in the United States, disrupted the Nation's financial markets and government operations, and caused billions of dollars in damage to the economy.

On September 14, 2001, the President declared a national emergency “by reason of the terrorist attacks at the World Trade Center, New York, New York, and the Pentagon, and the continuing and immediate threat of further attacks on the United States.” Proclamation No. 7463, 66 Fed. Reg. 48,199 (Sept. 14, 2001). The same day, Congress passed a joint resolution authorizing the President “to use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks” of September 11th, which the President signed on September 18th. AUMF § 2(a). Congress also expressly acknowledged that the attacks rendered it “necessary and appropriate” for the United States to exercise its right “to protect United States citizens both at home and abroad,” and in particular recognized that “the President has authority under the Constitution to take action to deter and prevent acts of international terrorism against the United States.” *Id.* pmb1. Congress emphasized that the attacks “continue to pose an unusual and extraordinary threat to the national security and foreign policy of the United States.” *Id.* The United States also launched a large-scale military response, both at home and abroad. In the United States, combat air patrols were immediately established over major metropolitan areas and were maintained 24 hours a day until April 2002. The United States also immediately began plans for a military response directed at al Qaeda’s base of operations in Afghanistan. Acting under his constitutional authority as Commander in Chief, and with the support of Congress, the President dispatched forces to Afghanistan and, with the assistance of the Northern Alliance, toppled the Taliban regime.

As the President made explicit in his Military Order of November 13, 2001, authorizing the use of military commissions to try terrorists, the attacks of September 11th “created a state of armed conflict.” Military Order § 1(a), 66 Fed. Reg. 57,833 (Nov. 13, 2001). Indeed, shortly after the attacks, NATO—for the first time in its 46-year history—invoked article 5 of the North Atlantic Treaty, which provides that an “armed attack against one or more of [the parties] shall be considered an attack against them all.” North Atlantic Treaty, Apr. 4, 1949, art. 5, 63 Stat. 2241, 2244, 34 U.N.T.S. 243, 246; *see also* Statement by NATO Secretary General Lord Robertson (Oct. 2, 2001), *available at* <http://www.nato.int/docu/speech/2001/s011002a.htm> (“[I]t has now been determined that the attack against the United States on 11 September was directed from abroad and shall therefore be regarded as an action covered by Article 5 of the Washington Treaty . . .”). The President also determined in his Military Order that al Qaeda and related terrorists organizations “possess both the capability and the intention to undertake further terrorist attacks against the United States that, if not detected and prevented, will cause mass deaths, mass injuries, and massive destruction of property, and may place at risk the continuity of the operations of the United States Government,” and concluded that “an extraordinary emergency exists for national defense purposes.” Military Order, § 1(c), (g), 66 Fed. Reg. at 57,833-34.

B. THE NSA ACTIVITIES

Against this unfolding background of events in the fall of 2001, there was substantial concern that al Qaeda and its allies were preparing to carry out another attack within the United States. Al Qaeda had demonstrated its ability to introduce agents into the United States undetected and to perpetrate devastating attacks, and it was suspected that additional agents were

likely already in position within the Nation's borders. As the President has explained, unlike a conventional enemy, al Qaeda has infiltrated "our cities and communities and communicated from here in America to plot and plan with bin Laden's lieutenants in Afghanistan, Pakistan and elsewhere." Press Conference of President Bush (Dec. 19, 2005), *available at* <http://www.whitehouse.gov/news/releases/2005/12/20051219-2.html> ("President's Press Conference"). To this day, finding al Qaeda sleeper agents in the United States remains one of the paramount concerns in the War on Terror. As the President has explained, "[t]he terrorists want to strike America again, and they hope to inflict even more damage than they did on September the 11th." *Id.*

The President has acknowledged that, to counter this threat, he has authorized the NSA to intercept international communications into and out of the United States of persons linked to al Qaeda or related terrorist organizations. The same day, the Attorney General elaborated and explained that in order to intercept a communication, there must be "a reasonable basis to conclude that one party to the communication is a member of al Qaeda, affiliated with al Qaeda, or a member of an organization affiliated with al Qaeda." Press Briefing by Attorney General Alberto Gonzales and General Michael Hayden, Principal Deputy Director for National Intelligence, *available at* <http://www.whitehouse.gov/news/releases/2005/12/20051219-1.html> (Dec. 19, 2005) (statement of Attorney General Gonzales). The purpose of these intercepts is to establish an early warning system to detect and prevent another catastrophic terrorist attack on the United States. The President has stated that the NSA activities "ha[ve] been effective in disrupting the enemy, while safeguarding our civil liberties." President's Press Conference.

The President has explained that the NSA activities are "critical" to the national security of the United States. *Id.* Confronting al Qaeda "is not simply a matter of [domestic] law enforcement"—we must defend the country against an enemy that declared war against the United States. *Id.* To "effectively detect enemies hiding in our midst and prevent them from striking us again . . . we must be able to act fast and to detect conversations [made by individuals linked to al Qaeda] so we can prevent new attacks." *Id.* The President pointed out that "a two-minute phone conversation between somebody linked to al Qaeda here and an operative overseas could lead directly to the loss of thousands of lives." *Id.* The NSA activities are intended to help "connect the dots" between potential terrorists. *Id.* In addition, the Nation is facing "a different era, a different war . . . people are changing phone numbers . . . and they're moving quick[ly]." *Id.* As the President explained, the NSA activities "enable[] us to move faster and quicker. And that's important. We've got to be fast on our feet, quick to detect and prevent." *Id.* "This is an enemy that is quick and it's lethal. And sometimes we have to move very, very quickly." *Id.* FISA, by contrast, is better suited "for long-term monitoring." *Id.*

As the President has explained, the NSA activities are "carefully reviewed approximately every 45 days to ensure that [they are] being used properly." *Id.* These activities are reviewed for legality by the Department of Justice and are monitored by the General Counsel and Inspector General of the NSA to ensure that civil liberties are being protected. *Id.* Leaders in Congress from both parties have been briefed more than a dozen times on the NSA activities.

C. THE CONTINUING THREAT POSED BY AL QAEDA

Before the September 11th attacks, al Qaeda had promised to attack the United States. In 1998, Osama bin Laden declared a “religious” war against the United States and urged that it was the moral obligation of all Muslims to kill U.S. civilians and military personnel. See Statement of Osama bin Laden, Ayman al-Zawahiri, et al., *Fatwah Urging Jihad Against Americans*, published in *Al-Quds al-'Arabi* (Feb. 23, 1998) (“To kill the Americans and their allies—civilians and military—is an individual duty for every Muslim who can do it in any country in which it is possible to do it, in order to liberate the al-Aqsa Mosque and the holy mosque from their grip, and in order for their armies to move out of all the lands of Islam, defeated and unable to threaten any Muslim.”). Al Qaeda carried out those threats with a vengeance; they attacked the U.S.S. Cole in Yemen, the United States Embassy in Nairobi, and finally the United States itself in the September 11th attacks.

It is clear that al Qaeda is not content with the damage it wrought on September 11th. As recently as December 7, 2005, Ayman al-Zawahiri professed that al Qaeda “is spreading, growing, and becoming stronger,” and that al Qaeda is “waging a great historic battle in Iraq, Afghanistan, Palestine, and even in the Crusaders’ own homes.” Ayman al-Zawahiri, videotape released on Al-Jazeera television network (Dec. 7, 2005). Indeed, since September 11th, al Qaeda leaders have repeatedly promised to deliver another, even more devastating attack on America. See, e.g., Osama bin Laden, videotape released on Al-Jazeera television network (Oct. 24, 2004) (warning United States citizens of further attacks and asserting that “your security is in your own hands”); Osama bin Laden, videotape released on Al-Jazeera television network (Oct. 18, 2003) (“We, God willing, will continue to fight you and will continue martyrdom operations inside and outside the United States”); Ayman Al-Zawahiri, videotape released on the Al-Jazeera television network (Oct. 9, 2002) (“I promise you [addressing the ‘citizens of the United States’] that the Islamic youth are preparing for you what will fill your hearts with horror”). Given that al Qaeda’s leaders have repeatedly made good on their threats and that al Qaeda has demonstrated its ability to insert foreign agents into the United States to execute attacks, it is clear that the threat continues. Indeed, since September 11th, al Qaeda has staged several large-scale attacks around the world, including in Indonesia, Madrid, and London, killing hundreds of innocent people.

ANALYSIS

I. THE PRESIDENT HAS INHERENT CONSTITUTIONAL AUTHORITY TO ORDER WARRANTLESS FOREIGN INTELLIGENCE SURVEILLANCE

As Congress expressly recognized in the AUMF, “the President has authority under the Constitution to take action to deter and prevent acts of international terrorism against the United States,” AUMF pmb1., especially in the context of the current conflict. Article II of the Constitution vests in the President all executive power of the United States, including the power to act as Commander in Chief of the Armed Forces, see U.S. Const. art. II, § 2, and authority over the conduct of the Nation’s foreign affairs. As the Supreme Court has explained, “[t]he President is the sole organ of the nation in its external relations, and its sole representative with

foreign nations.” *United States v. Curtiss-Wright Export Corp.*, 299 U.S. 304, 319 (1936) (internal quotation marks and citations omitted). In this way, the Constitution grants the President inherent power to protect the Nation from foreign attack, *see, e.g., The Prize Cases*, 67 U.S. (2 Black) 635, 668 (1863), and to protect national security information, *see, e.g., Department of the Navy v. Egan*, 484 U.S. 518, 527 (1988).

To carry out these responsibilities, the President must have authority to gather information necessary for the execution of his office. The Founders, after all, intended the federal Government to be clothed with all authority necessary to protect the Nation. *See, e.g., The Federalist* No. 23, at 147 (Alexander Hamilton) (Jacob E. Cooke ed. 1961) (explaining that the federal Government will be “cloathed with all the powers requisite to the complete execution of its trust”); *id.* No. 41, at 269 (James Madison) (“Security against foreign danger is one of the primitive objects of civil society The powers requisite for attaining it must be effectually confided to the federal councils.”). Because of the structural advantages of the Executive Branch, the Founders also intended that the President would have the primary responsibility and necessary authority as Commander in Chief and Chief Executive to protect the Nation and to conduct the Nation’s foreign affairs. *See, e.g., The Federalist* No. 70, at 471-72 (Alexander Hamilton); *see also Johnson v. Eisentrager*, 339 U.S. 763, 788 (1950) (“this [constitutional] grant of war power includes all that is necessary and proper for carrying these powers into execution”) (citation omitted). Thus, it has been long recognized that the President has the authority to use secretive means to collect intelligence necessary for the conduct of foreign affairs and military campaigns. *See, e.g., Chicago & S. Air Lines v. Waterman S.S. Corp.*, 333 U.S. 103, 111 (1948) (“The President, both as Commander-in-Chief and as the Nation’s organ for foreign affairs, has available intelligence services whose reports are not and ought not to be published to the world.”); *Curtiss-Wright*, 299 U.S. at 320 (“He has his confidential sources of information. He has his agents in the form of diplomatic, consular and other officials.”); *Totten v. United States*, 92 U.S. 105, 106 (1876) (President “was undoubtedly authorized during the war, as commander-in-chief . . . to employ secret agents to enter the rebel lines and obtain information respecting the strength, resources, and movements of the enemy”).

In reliance on these principles, a consistent understanding has developed that the President has inherent constitutional authority to conduct warrantless searches and surveillance within the United States for foreign intelligence purposes. Wiretaps for such purposes thus have been authorized by Presidents at least since the administration of Franklin Roosevelt in 1940. *See, e.g., United States v. United States District Court*, 444 F.2d 651, 669-71 (6th Cir. 1971) (reproducing as an appendix memoranda from Presidents Roosevelt, Truman, and Johnson). In a Memorandum to Attorney General Jackson, President Roosevelt wrote on May 21, 1940:

You are, therefore, authorized and directed in such cases as you may approve, after investigation of the need in each case, to authorize the necessary investigation agents that they are at liberty to secure information by listening devices directed to the conversation or other communications of persons suspected of subversive activities against the Government of the United States, including suspected spies. You are requested furthermore to limit these investigations so conducted to a minimum and limit them insofar as

possible to aliens.

Id. at 670 (appendix A). President Truman approved a memorandum drafted by Attorney General Tom Clark in which the Attorney General advised that “it is as necessary as it was in 1940 to take the investigative measures” authorized by President Roosevelt to conduct electronic surveillance “in cases vitally affecting the domestic security.” *Id.* Indeed, while FISA was being debated during the Carter Administration, Attorney General Griffin Bell testified that “the current bill recognizes no inherent power of the President to conduct electronic surveillance, and I want to interpolate here to say that *this does not take away the power [of] the President under the Constitution.*” Foreign Intelligence Electronic Surveillance Act of 1978: Hearings on H.R. 5764, H.R. 9745, H.R. 7308, and H.R. 5632 Before the Subcomm. on Legislation of the House Comm. on Intelligence, 95th Cong., 2d Sess. 15 (1978) (emphasis added); *see also Katz v. United States*, 389 U.S. 347, 363 (1967) (White, J., concurring) (“Wiretapping to protect the security of the Nation has been authorized by successive Presidents.”); *cf.* Amending the Foreign Intelligence Surveillance Act: Hearings Before the House Permanent Select Comm. on Intelligence, 103d Cong. 2d Sess. 61 (1994) (statement of Deputy Attorney General Jamie S. Gorelick) (“[T]he Department of Justice believes, and the case law supports, that the President has inherent authority to conduct warrantless physical searches for foreign intelligence purposes . . .”).

The courts uniformly have approved this longstanding Executive Branch practice. Indeed, every federal appellate court to rule on the question has concluded that, even in peacetime, the President has inherent constitutional authority, consistent with the Fourth Amendment, to conduct searches for foreign intelligence purposes without securing a judicial warrant. *See In re Sealed Case*, 310 F.3d 717, 742 (Foreign Intel. Surv. Ct. of Rev. 2002) (“[A]ll the other courts to have decided the issue [have] held that the President did have inherent authority to conduct warrantless searches to obtain foreign intelligence information *We take for granted that the President does have that authority and, assuming that is so, FISA could not encroach on the President's constitutional power.*”) (emphasis added); *accord, e.g., United States v. Truong Dinh Hung*, 629 F.2d 908 (4th Cir. 1980); *United States v. Butenko*, 494 F.2d 593 (3d Cir. 1974) (en banc); *United States v. Brown*, 484 F.2d 418 (5th Cir. 1973). *But cf. Zweibon v. Mitchell*, 516 F.2d 594 (D.C. Cir. 1975) (en banc) (dictum in plurality opinion suggesting that a warrant would be required even in a foreign intelligence investigation).

In *United States v. United States District Court*, 407 U.S. 297 (1972) (the “*Keith*” case), the Supreme Court concluded that the Fourth Amendment’s warrant requirement applies to investigations of wholly *domestic* threats to security—such as domestic political violence and other crimes. But the Court in the *Keith* case made clear that it was not addressing the President’s authority to conduct *foreign* intelligence surveillance without a warrant and that it was expressly reserving that question: “[T]he instant case requires no judgment on the scope of the President’s surveillance power with respect to the activities of foreign powers, within or without this country.” *Id.* at 308; *see also id.* at 321-22 & n.20 (“We have not addressed, and express no opinion as to, the issues which may be involved with respect to activities of foreign powers or their agents.”). That *Keith* does not apply in the context of protecting against a foreign attack has been confirmed by the lower courts. After *Keith*, each of the three courts of appeals

that have squarely considered the question have concluded—expressly taking the Supreme Court’s decision into account—that the President has inherent authority to conduct warrantless surveillance in the foreign intelligence context. *See, e.g., Truong Dinh Hung*, 629 F.2d at 913-14; *Butenko*, 494 F.2d at 603; *Brown*, 484 F.2d 425-26.

From a constitutional standpoint, foreign intelligence surveillance such as the NSA activities differs fundamentally from the domestic security surveillance at issue in *Keith*. As the Fourth Circuit observed, the President has uniquely strong constitutional powers in matters pertaining to foreign affairs and national security. “Perhaps most crucially, the executive branch not only has superior expertise in the area of foreign intelligence, it is also constitutionally designated as the pre-eminent authority in foreign affairs.” *Truong*, 629 F.2d at 914; *see id.* at 913 (noting that “the needs of the executive are so compelling in the area of foreign intelligence, unlike the area of domestic security, that a uniform warrant requirement would . . . unduly frustrate the President in carrying out his foreign affairs responsibilities”); *cf. Haig v. Agee*, 453 U.S. 280, 292 (1981) (“Matters intimately related to foreign policy and national security are rarely proper subjects for judicial intervention.”).²

The present circumstances that support recognition of the President’s inherent constitutional authority to conduct the NSA activities are considerably stronger than were the circumstances at issue in the earlier courts of appeals cases that recognized this power. All of the cases described above addressed inherent executive authority under the foreign affairs power to conduct surveillance in a peacetime context. The courts in these cases therefore had no occasion even to consider the fundamental authority of the President, as Commander in Chief, to gather intelligence in the context of an ongoing armed conflict in which the United States already had suffered massive civilian casualties and in which the intelligence gathering efforts at issue were specifically designed to thwart further armed attacks. Indeed, intelligence gathering is particularly important in the current conflict, in which the enemy attacks largely through clandestine activities and which, as Congress recognized, “pose[s] an unusual and extraordinary threat,” AUMF pmbl.

Among the President’s most basic constitutional duties is the duty to protect the Nation from armed attack. The Constitution gives him all necessary authority to fulfill that responsibility. The courts thus have long acknowledged the President’s inherent authority to take action to protect Americans abroad, *see, e.g., Durand v. Hollins*, 8 F. Cas. 111, 112 (C.C.S.D.N.Y. 1866) (No. 4186), and to protect the Nation from attack, *see, e.g., The Prize Cases*, 67 U.S. at 668. *See generally Ex parte Quirin*, 317 U.S. 1, 28 (1942) (recognizing that

² *Keith* made clear that one of the significant concerns driving the Court’s conclusion in the domestic security context was the inevitable connection between perceived threats to domestic security and political dissent. As the Court explained: “Fourth Amendment protections become the more necessary when the targets of official surveillance may be those suspected of unorthodoxy in their political beliefs. The danger to political dissent is acute where the Government attempts to act under so vague a concept as the power to protect ‘domestic security.’” *Keith*, 407 U.S. at 314; *see also id.* at 320 (“Security surveillances are especially sensitive because of the inherent vagueness of the domestic security concept, the necessarily broad and continuing nature of intelligence gathering, and the temptation to utilize such surveillances to oversee political dissent.”). Surveillance of domestic groups raises a First Amendment concern that generally is not present when the subjects of the surveillance are foreign powers or their agents.

the President has authority under the Constitution “to direct the performance of those functions which may constitutionally be performed by the military arm of the nation in time of war,” including “important incident[s] to the conduct of war,” such as “the adoption of measures by the military command . . . to repel and defeat the enemy”). As the Supreme Court emphasized in the *Prize Cases*, if the Nation is invaded, the President is “bound to resist force by force”; “[h]e must determine what degree of force the crisis demands” and need not await congressional sanction to do so. *The Prize Cases*, 67 U.S. at 670; see also *Campbell v. Clinton*, 203 F.3d 19, 27 (D.C. Cir. 2000) (Silberman, J., concurring) (“[T]he *Prize Cases* . . . stand for the proposition that the President has independent authority to repel aggressive acts by third parties even without specific congressional authorization, and courts may not review the level of force selected.”); *id.* at 40 (Tatel, J., concurring) (“[T]he President, as commander in chief, possesses emergency authority to use military force to defend the nation from attack without obtaining prior congressional approval.”). Indeed, “in virtue of his rank as head of the forces, [the President] has certain powers and duties with which Congress cannot interfere.” *Training of British Flying Students in the United States*, 40 Op. Att’y Gen. 58, 61 (1941) (Attorney General Robert H. Jackson) (internal quotation marks omitted). In exercising his constitutional powers, the President has wide discretion, consistent with the Constitution, over the methods of gathering intelligence about the Nation’s enemies in a time of armed conflict.

II. THE AUMF CONFIRMS AND SUPPLEMENTS THE PRESIDENT’S INHERENT POWER TO USE WARRANTLESS SURVEILLANCE AGAINST THE ENEMY IN THE CURRENT ARMED CONFLICT

In the Authorization for Use of Military Force enacted in the wake of September 11th, Congress confirms and supplements the President’s constitutional authority to protect the Nation, including through electronic surveillance, in the context of the current post-September 11th armed conflict with al Qaeda and its allies. The broad language of the AUMF affords the President, at a minimum, discretion to employ the traditional incidents of the use of military force. The history of the President’s use of warrantless surveillance during armed conflicts demonstrates that the NSA surveillance described by the President is a fundamental incident of the use of military force that is necessarily included in the AUMF.

A. THE TEXT AND PURPOSE OF THE AUMF AUTHORIZE THE NSA ACTIVITIES

On September 14, 2001, in its first legislative response to the attacks of September 11th, Congress gave its express approval to the President’s military campaign against al Qaeda and, in the process, confirmed the well-accepted understanding of the President’s Article II powers. See AUMF § 2(a).³ In the preamble to the AUMF, Congress stated that “the President has authority under the Constitution to take action to deter and prevent acts of international terrorism against the United States,” AUMF pmbl., and thereby acknowledged the President’s inherent constitutional authority to defend the United States. This clause “constitutes an extraordinarily

³ America’s military response began before the attacks of September 11th had been completed. See *The 9/11 Commission Report 20* (2004). Combat air patrols were established and authorized “to engage inbound aircraft if they could verify that the aircraft was hijacked.” *Id.* at 42.

sweeping recognition of independent presidential *constitutional* power to employ the war power to combat terrorism.” Michael Stokes Paulsen, *Youngstown Goes to War*, 19 Const. Comment. 215, 252 (2002). This striking recognition of presidential authority cannot be discounted as the product of excitement in the immediate aftermath of September 11th, for the same terms were repeated by Congress more than a year later in the Authorization for Use of Military Force Against Iraq Resolution of 2002. Pub. L. No. 107-243, pmb1., 116 Stat. 1498, 1500 (Oct. 16, 2002) (“[T]he President has authority under the Constitution to take action in order to deter and prevent acts of international terrorism against the United States . . .”). In the context of the conflict with al Qaeda and related terrorist organizations, therefore, Congress has acknowledged a broad executive authority to “deter and prevent” further attacks against the United States.

The AUMF passed by Congress on September 14, 2001, does not lend itself to a narrow reading. Its expansive language authorizes 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 that occurred on September 11, 2001.” AUMF § 2(a) (emphases added). In the field of foreign affairs, and particularly that of war powers and national security, congressional enactments are to be broadly construed where they indicate support for authority long asserted and exercised by the Executive Branch. *See, e.g., Haig v. Agee*, 453 U.S. 280, 293-303 (1981); *United States ex rel. Knauff v. Shaughnessy*, 338 U.S. 537, 543-45 (1950); *cf. Loving v. United States*, 517 U.S. 748, 772 (1996) (noting that the usual “limitations on delegation [of congressional powers] do not apply” to authorizations linked to the Commander in Chief power); *Dames & Moore v. Regan*, 453 U.S. 654, 678-82 (1981) (even where there is no express statutory authorization for executive action, legislation in related field may be construed to indicate congressional acquiescence in that action). Although Congress’s war powers under Article I, Section 8 of the Constitution empower Congress to legislate regarding the raising, regulation, and material support of the Armed Forces and related matters, rather than the prosecution of military campaigns, the AUMF indicates Congress’s endorsement of the President’s use of his constitutional war powers. This authorization transforms the struggle against al Qaeda and related terrorist organizations from what Justice Jackson called “a zone of twilight,” in which the President and the Congress may have concurrent powers whose “distribution is uncertain,” *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 637 (1952) (Jackson, J., concurring), into a situation in which the President’s authority is at its maximum because “it includes all that he possesses in his own right plus all that Congress can delegate,” *id.* at 635. With regard to these fundamental tools of warfare—and, as demonstrated below, warrantless electronic surveillance against the declared enemy is one such tool—the AUMF places the President’s authority at its zenith under *Youngstown*.

It is also clear that the AUMF confirms and supports the President’s use of those traditional incidents of military force against the enemy, wherever they may be—on United States soil or abroad. The nature of the September 11th attacks—launched on United States soil by foreign agents secreted in the United States—necessitates such authority, and the text of the AUMF confirms it. The operative terms of the AUMF state that the President is authorized to use force “in order to prevent any future acts of international terrorism against the United States,” *id.*, an objective which, given the recent attacks within the Nation’s borders and the continuing use of air defense throughout the country at the time Congress acted, undoubtedly

contemplated the possibility of military action within the United States. The preamble, moreover, recites that the United States should exercise its rights “to protect United States citizens both *at home* and abroad.” *Id.* pmbl. (emphasis added). To take action against those linked to the September 11th attacks involves taking action against individuals within the United States. The United States had been attacked on its own soil—not by aircraft launched from carriers several hundred miles away, but by enemy agents who had resided in the United States for months. A crucial responsibility of the President—charged by the AUMF and the Constitution—was and is to identify and attack those enemies, especially if they were in the United States, ready to strike against the Nation.

The text of the AUMF demonstrates in an additional way that Congress authorized the President to conduct warrantless electronic surveillance against the enemy. The terms of the AUMF not only authorized the President to “use all necessary and appropriate force” against those responsible for the September 11th attacks; it also authorized the President to “determine[]” the persons or groups responsible for those attacks and to take all actions necessary to prevent further attacks. AUMF § 2(a) (“the President is authorized to use all necessary and appropriate force against those nations, organizations, or persons *he determines* planned, authorized, committed, or aided the terrorist attacks that occurred on September 11th, 2001, or harbored such organizations or persons”) (emphasis added). Of vital importance to the use of force against the enemy is locating the enemy and identifying its plans of attack. And of vital importance to identifying the enemy and detecting possible future plots was the authority to intercept communications to or from the United States of persons with links to al Qaeda or related terrorist organizations. Given that the agents who carried out the initial attacks resided in the United States and had successfully blended into American society and disguised their identities and intentions until they were ready to strike, the necessity of using the most effective intelligence gathering tools against such an enemy, including electronic surveillance, was patent. Indeed, Congress recognized that the enemy in this conflict poses an “unusual and extraordinary threat.” AUMF pmbl.

The Supreme Court’s interpretation of the scope of the AUMF in *Hamdi v. Rumsfeld*, 542 U.S. 507 (2004), strongly supports this reading of the AUMF. In *Hamdi*, five members of the Court found that the AUMF authorized the detention of an American within the United States, notwithstanding a statute that prohibits the detention of U.S. citizens “except pursuant to an Act of Congress,” 18 U.S.C. § 4001(a). *See Hamdi*, 542 U.S. at 519 (plurality opinion); *id.* at 587 (Thomas, J., dissenting). Drawing on historical materials and “longstanding law-of-war principles,” *id.* at 518-21, a plurality of the Court concluded that detention of combatants who fought against the United States as part of an organization “known to have supported” al Qaeda “is so fundamental and accepted an incident to war as to be an exercise of the ‘necessary and appropriate force’ Congress has authorized the President to use.” *Id.* at 518; *see also id.* at 587 (Thomas, J., dissenting) (agreeing with the plurality that the joint resolution authorized the President to “detain those arrayed against our troops”); *accord Quirin*, 317 U.S. at 26-29, 38 (recognizing the President’s authority to capture and try agents of the enemy in the United States even if they had never “entered the theatre or zone of active military operations”). Thus, even though the AUMF does not say anything expressly about detention, the Court nevertheless found that it satisfied section 4001(a)’s requirement that detention be congressionally authorized.

The conclusion of five Justices in *Hamdi* that the AUMF incorporates fundamental “incidents” of the use of military force makes clear that the absence of any specific reference to signals intelligence activities in the resolution is immaterial. See *Hamdi*, 542 U.S. at 519 (“[I]t is of no moment that the AUMF does not use specific language of detention.”) (plurality opinion). Indeed, given the circumstances in which the AUMF was adopted, it is hardly surprising that Congress chose to speak about the President’s authority in general terms. The purpose of the AUMF was for Congress to sanction and support the military response to the devastating terrorist attacks that had occurred just three days earlier. Congress evidently thought it neither necessary nor appropriate to attempt to catalog every specific aspect of the use of the forces it was authorizing and every potential preexisting statutory limitation on the Executive Branch. Rather than engage in that difficult and impractical exercise, Congress authorized the President, in general but intentionally broad terms, to use the traditional and fundamental incidents of war and to determine how best to identify and engage the enemy in the current armed conflict. Congress’s judgment to proceed in this manner was unassailable, for, as the Supreme Court has recognized, even in normal times involving no major national security crisis, “Congress cannot anticipate and legislate with regard to every possible action the President may find it necessary to take.” *Dames & Moore*, 453 U.S. at 678. Indeed, Congress often has enacted authorizations to use military force using general authorizing language that does not purport to catalogue in detail the specific powers the President may employ. The need for Congress to speak broadly in recognizing and augmenting the President’s core constitutional powers over foreign affairs and military campaigns is of course significantly heightened in times of national emergency. See *Zemel v. Rusk*, 381 U.S. 1, 17 (1965) (“[B]ecause of the changeable and explosive nature of contemporary international relations . . . Congress—in giving the Executive authority over matters of foreign affairs—must of necessity paint with a brush broader than that it customarily wields in domestic areas.”).

Hamdi thus establishes the proposition that the AUMF “clearly and unmistakably” authorizes the President to take actions against al Qaeda and related organizations that amount to “fundamental incident[s] of waging war.” *Hamdi*, 542 U.S. at 519 (plurality opinion); see also *id.* at 587 (Thomas, J., dissenting). In other words, “[t]he clear inference is that the AUMF authorizes what the laws of war permit.” Curtis A. Bradley & Jack L. Goldsmith, *Congressional Authorization and the War on Terrorism*, 118 Harv. L. Rev. 2048, 2092 (2005) (emphasis added). Congress is presumed to be aware of the Supreme Court’s precedents. Indeed, Congress recently enacted legislation in response to the Court’s decision in *Rasul v. Bush*, 542 U.S. 466 (2004)—which was issued the same day as the *Hamdi* decision—removing habeas corpus jurisdiction over claims filed on behalf of confined enemy combatants held at Guantanamo Bay. Congress, however, has not expressed any disapproval of the Supreme Court’s commonsense and plain-meaning interpretation of the AUMF in *Hamdi*.⁴

⁴ This understanding of the AUMF is consistent with Justice O’Connor’s admonition that “a state of war is not a blank check for the President,” *Hamdi*, 542 U.S. at 536 (plurality opinion). In addition to constituting a fundamental and accepted incident of the use of military force, the NSA activities are consistent with the law of armed conflict principle that the use of force be necessary and proportional. See Dieter Fleck, *The Handbook of Humanitarian Law in Armed Conflicts* 115 (1995). The NSA activities are proportional because they are minimally invasive and narrow in scope, targeting only the international communications of persons reasonably believed to be linked to al Qaeda, and are designed to protect the Nation from a devastating attack.

B. WARRANTLESS ELECTRONIC SURVEILLANCE AIMED AT INTERCEPTING ENEMY COMMUNICATIONS HAS LONG BEEN RECOGNIZED AS A FUNDAMENTAL INCIDENT OF THE USE OF MILITARY FORCE

The history of warfare—including the consistent practice of Presidents since the earliest days of the Republic—demonstrates that warrantless intelligence surveillance against the enemy is a fundamental incident of the use of military force, and this history confirms the statutory authority provided by the AUMF. Electronic surveillance is a fundamental tool of war that must be included in any natural reading of the AUMF’s authorization to use “all necessary and appropriate force.”

As one author has explained:

It is *essential* in warfare for a belligerent to be as fully informed as possible about the enemy—his strength, his weaknesses, measures taken by him and measures contemplated by him. This applies not only to military matters, but . . . anything which bears on and is material to his ability to wage the war in which he is engaged. *The laws of war recognize and sanction this aspect of warfare.*

Morris Greenspan, *The Modern Law of Land Warfare* 325 (1959) (emphases added); *see also* Memorandum for Members of the House Permanent Select Comm. on Intel., from Jeffrey H. Smith, *Re: Legal Authorities Regarding Warrantless Surveillance of U.S. Persons* 6 (Jan. 3, 2006) (“Certainly, the collection of intelligence is understood to be necessary to the execution of the war.”). Similarly, article 24 of the Hague Regulations of 1907 expressly states that “the employment of measures necessary for obtaining information about the enemy and the country [is] considered permissible.” *See also* L. Oppenheim, *International Law* vol. II § 159 (7th ed. 1952) (“War cannot be waged without all kinds of information, about the forces and the intentions of the enemy To obtain the necessary information, it has always been considered lawful to employ spies”); Joseph R. Baker & Henry G. Crocker, *The Laws of Land Warfare* 197 (1919) (“Every belligerent has a right . . . to discover the signals of the enemy and . . . to seek to procure information regarding the enemy through the aid of secret agents.”); *cf.* J.M. Spaight, *War Rights on Land* 205 (1911) (“[E]very nation employs spies; were a nation so quixotic as to refrain from doing so, it might as well sheathe its sword for ever. . . . Spies . . . are indispensably necessary to a general; and, other things being equal, that commander will be victorious who has the best secret service.”) (internal quotation marks omitted).

In accordance with these well-established principles, the Supreme Court has consistently recognized the President’s authority to conduct intelligence activities. *See, e.g., Totten v. United States*, 92 U.S. 105, 106 (1876) (recognizing President’s authority to hire spies); *Tenei v. Doe*, 544 U.S. 1 (2005) (reaffirming *Totten* and counseling against judicial interference with such matters); *see also Chicago & S. Air Lines v. Waterman S.S. Corp.*, 333 U.S. 103, 111 (1948) (“The President, both as Commander-in-Chief and as the Nation’s organ for foreign affairs, has available intelligence services whose reports neither are not and ought not to be published to the world.”); *United States v. Curtiss-Wright Export Corp.*, 299 U.S. 304, 320 (1936) (The President “has his confidential sources of information. He has his agents in the form of diplomatic,

consular, and other officials.”). Chief Justice John Marshall even described the gathering of intelligence as a military duty. See *Tatum v. Laird*, 444 F.2d 947, 952-53 (D.C. Cir. 1971) (“As Chief Justice John Marshall said of Washington, ‘A general must be governed by his intelligence and must regulate his measures by his information. It is his duty to obtain correct information’”) (quoting Foreword, U.S. Army Basic Field Manual, Vol. X, circa 1938), *rev’d on other grounds*, 408 U.S. 1 (1972).

The United States, furthermore, has a long history of wartime surveillance—a history that can be traced to George Washington, who “was a master of military espionage” and “made frequent and effective use of secret intelligence in the second half of the eighteenth century.” Rhodri Jeffreys-Jones, *Cloak and Dagger: A History of American Secret Intelligence* 11 (2002); see generally *id.* at 11-23 (recounting Washington’s use of intelligence); see also *Haig v. Agee*, 471 U.S. 159, 172 n.16 (1981) (quoting General Washington’s letter to an agent embarking upon an intelligence mission in 1777: “The necessity of procuring good intelligence, is apparent and need not be further urged.”). As President in 1790, Washington obtained from Congress a “secret fund” to deal with foreign dangers and to be spent at his discretion. Jeffreys-Jones, *supra*, at 22. The fund, which remained in use until the creation of the Central Intelligence Agency in the mid-twentieth century and gained “longstanding acceptance within our constitutional structure,” *Halperin v. CIA*, 629 F.2d 144, 158-59 (D.C. Cir. 1980), was used “for all purposes to which a secret service fund should or could be applied for the public benefit,” including “for persons sent publicly and secretly to search for important information, political or commercial,” *id.* at 159 (quoting Statement of Senator John Forsyth, Cong. Debates 295 (Feb. 25, 1831)). See also *Totten*, 92 U.S. at 107 (refusing to examine payments from this fund lest the publicity make a “secret service” “impossible”).

The interception of communications, in particular, has long been accepted as a fundamental method for conducting wartime surveillance. See, e.g., Greenspan, *supra*, at 326 (accepted and customary means for gathering intelligence “include air reconnaissance and photography; ground reconnaissance; observation of enemy positions; *interception of enemy messages, wireless and other*; examination of captured documents; . . . and interrogation of prisoners and civilian inhabitants”) (emphasis added). Indeed, since its independence, the United States has intercepted communications for wartime intelligence purposes and, if necessary, has done so within its own borders. During the Revolutionary War, for example, George Washington received and used to his advantage reports from American intelligence agents on British military strength, British strategic intentions, and British estimates of American strength. See Jeffreys-Jones, *supra*, at 13. One source of Washington’s intelligence was intercepted British mail. See Central Intelligence Agency, *Intelligence in the War of Independence* 31, 32 (1997). In fact, Washington himself proposed that one of his Generals “contrive a means of opening [British letters] without breaking the seals, take copies of the contents, and then let them go on.” *Id.* at 32 (“From that point on, Washington was privy to British intelligence pouches between New York and Canada.”); see generally Final Report of the Select Committee to Study Governmental Operations with respect to Intelligence Activities (the “Church Committee”), S. Rep. No. 94-755, at Book VI, 9-17 (Apr. 23, 1976) (describing Washington’s intelligence activities).

More specifically, warrantless electronic surveillance of wartime communications has been conducted in the United States since electronic communications have existed, *i.e.*, since at least the Civil War, when “[t]elegraph wiretapping was common, and an important intelligence source for both sides.” G.J.A. O’Toole, *The Encyclopedia of American Intelligence and Espionage* 498 (1988). Confederate General J.E.B. Stuart even “had his own personal wiretapper travel along with him in the field” to intercept military telegraphic communications. Samuel Dash, et al., *The Eavesdroppers* 23 (1971); *see also* O’Toole, *supra*, at 121, 385-88, 496-98 (discussing Civil War surveillance methods such as wiretaps, reconnaissance balloons, semaphore interception, and cryptanalysis). Similarly, there was extensive use of electronic surveillance during the Spanish-American War. *See* Bruce W. Bidwell, *History of the Military Intelligence Division, Department of the Army General Staff: 1775-1941*, at 62 (1986). When an American expeditionary force crossed into northern Mexico to confront the forces of Pancho Villa in 1916, the Army “frequently intercepted messages of the regime in Mexico City or the forces contesting its rule.” David Alvarez, *Secret Messages* 6-7 (2000). Shortly after Congress declared war on Germany in World War I, President Wilson (citing only his constitutional powers and the joint resolution declaring war) ordered the censorship of messages sent outside the United States via submarine cables, telegraph, and telephone lines. *See* Exec. Order No. 2604 (Apr. 28, 1917). During that war, wireless telegraphy “enabled each belligerent to tap the messages of the enemy.” Bidwell, *supra*, at 165 (quoting statement of Col. W. Nicolai, former head of the Secret Service of the High Command of the German Army, *in* W. Nicolai, *The German Secret Service* 21 (1924)).

As noted in Part I, on May 21, 1940, President Roosevelt authorized warrantless electronic surveillance of persons suspected of subversive activities, including spying, against the United States. In addition, on December 8, 1941, the day after the attack on Pearl Harbor, President Roosevelt gave the Director of the FBI “temporary powers to direct all news censorship and to control all other telecommunications traffic in and out of the United States.” Jack A. Gottschalk, “Consistent with Security”. . . . *A History of American Military Press Censorship*, 5 Comm. & L. 35, 39 (1983) (emphasis added). *See* Memorandum for the Secretaries of War, Navy, State, and Treasury, the Postmaster General, and the Federal Communications Commission from Franklin D. Roosevelt (Dec. 8, 1941). President Roosevelt soon supplanted that temporary regime by establishing an office for conducting such electronic surveillance in accordance with the War Powers Act of 1941. *See* Pub. L. No. 77-354, § 303, 55 Stat. 838, 840-41 (Dec. 18, 1941); Gottschalk, 5 Comm. & L. at 40. The President’s order gave the Government of the United States access to “communications by mail, cable, radio, or other means of transmission passing between the United States and any foreign country.” *Id.* *See also* Exec. Order No. 8985, § 1, 6 Fed. Reg. 6625, 6625 (Dec. 19, 1941). In addition, the United States systematically listened surreptitiously to electronic communications as part of the war effort. *See* Dash, *Eavesdroppers* at 30. During World War II, signals intelligence assisted in, among other things, the destruction of the German U-boat fleet by the Allied naval forces, *see id.* at 27, and the war against Japan, *see* O’Toole, *supra*, at 32, 323-24. In general, signals intelligence “helped to shorten the war by perhaps two years, reduce the loss of life, and make inevitable an eventual Allied victory.” Carl Boyd, *American Command of the Sea Through Carriers, Codes, and the Silent Service: World War II and Beyond* 27 (1995); *see also* Alvarez, *supra*, at 1 (“There can be little doubt that signals intelligence contributed significantly to the

military defeat of the Axis.”). Significantly, not only was wiretapping in World War II used “extensively by military intelligence and secret service personnel in combat areas abroad,” but also “by the FBI and secret service in this country.” Dash, *supra*, at 30.

In light of the long history of prior wartime practice, the NSA activities fit squarely within the sweeping terms of the AUMF. The use of signals intelligence to identify and pinpoint the enemy is a traditional component of wartime military operations—or, to use the terminology of *Hamdi*, a “fundamental and accepted . . . incident to war,” 542 U.S. at 518 (plurality opinion)—employed to defeat the enemy and to prevent enemy attacks in the United States. Here, as in other conflicts, the enemy may use public communications networks, and some of the enemy may already be in the United States. Although those factors may be present in this conflict to a greater degree than in the past, neither is novel. Certainly, both factors were well known at the time Congress enacted the AUMF. Wartime interception of international communications made by the enemy thus should be understood, no less than the wartime detention at issue in *Hamdi*, as one of the basic methods of engaging and defeating the enemy that Congress authorized in approving “*all necessary and appropriate force*” that the President would need to defend the Nation. AUMF § 2(a) (emphasis added).

* * *

Accordingly, the President has the authority to conduct warrantless electronic surveillance against the declared enemy of the United States in a time of armed conflict. That authority derives from the Constitution, and is reinforced by the text and purpose of the AUMF, the nature of the threat posed by al Qaeda that Congress authorized the President to repel, and the long-established understanding that electronic surveillance is a fundamental incident of the use of military force. The President’s power in authorizing the NSA activities is at its zenith because he has acted “pursuant to an express or implied authorization of Congress.” *Youngstown*, 343 U.S. at 635 (Jackson, J., concurring).

III. THE NSA ACTIVITIES ARE CONSISTENT WITH THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

The President’s exercise of his constitutional authority to conduct warrantless wartime electronic surveillance of the enemy, as confirmed and supplemented by statute in the AUMF, is fully consistent with the requirements of the Foreign Intelligence Surveillance Act (“FISA”).⁵ FISA is a critically important tool in the War on Terror. The United States makes full use of the authorities available under FISA to gather foreign intelligence information, including authorities to intercept communications, conduct physical searches, and install and use pen registers and trap and trace devices. While FISA establishes certain procedures that must be followed for these authorities to be used (procedures that usually involve applying for and obtaining an order from a special court), FISA also expressly contemplates that a later legislative enactment could

⁵ To avoid revealing details about the operation of the program, it is assumed for purposes of this paper that the activities described by the President constitute “electronic surveillance,” as defined by FISA; 50 U.S.C. § 1801(f).

authorize electronic surveillance outside the procedures set forth in FISA itself. The AUMF constitutes precisely such an enactment. To the extent there is any ambiguity on this point, the canon of constitutional avoidance requires that such ambiguity be resolved in favor of the President's authority to conduct the communications intelligence activities he has described. Finally, if FISA could not be read to allow the President to authorize the NSA activities during the current congressionally authorized armed conflict with al Qaeda, FISA would be unconstitutional as applied in this narrow context.

A. THE REQUIREMENTS OF FISA

FISA was enacted in 1978 to regulate "electronic surveillance," particularly when conducted to obtain "foreign intelligence information," as those terms are defined in section 101 of FISA, 50 U.S.C. § 1801. As a general matter, the statute requires that the Attorney General approve an application for an order from a special court composed of Article III judges and created by FISA—the Foreign Intelligence Surveillance Court ("FISC"). *See* 50 U.S.C. §§ 1803-1804. The application must demonstrate, among other things, that there is probable cause to believe that the target is a foreign power or an agent of a foreign power. *See id.* § 1805(a)(3)(A). It must also contain a certification from the Assistant to the President for National Security Affairs or an officer of the United States appointed by the President with the advice and consent of the Senate and having responsibilities in the area of national security or defense that the information sought is foreign intelligence information and cannot reasonably be obtained by normal investigative means. *See id.* § 1804(a)(7). FISA further requires the Government to state the means that it proposes to use to obtain the information and the basis for its belief that the facilities at which the surveillance will be directed are being used or are about to be used by a foreign power or an agent of a foreign power. *See id.* § 1804(a)(4), (a)(8).

FISA was the first congressional measure that sought to impose restrictions on the Executive Branch's authority to engage in electronic surveillance for foreign intelligence purposes, an authority that, as noted above, had been repeatedly recognized by the federal courts. *See* Americo R. Cinquegrana, *The Walls (and Wires) Have Ears: The Background and First Ten Years of the Foreign Intelligence Surveillance Act of 1978*, 137 U. Penn. L. Rev. 793, 810 (1989) (stating that the "status of the President's inherent authority" to conduct surveillance "formed the core of subsequent legislative deliberations" leading to the enactment of FISA). To that end, FISA modified a provision in Title III that previously had disclaimed any intent to have laws governing wiretapping interfere with the President's constitutional authority to gather foreign intelligence. Prior to the passage of FISA, section 2511(3) of title 18 had stated that "[n]othing contained in this chapter or in section 605 of the Communications Act of 1934 . . . shall limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities." 18 U.S.C. § 2511(3) (1970). FISA replaced that provision with an important, though more limited, preservation of authority for the President. *See* Pub. L. No. 95-511, § 201(b), (c), 92 Stat. 1783, 1797 (1978), codified at 18 U.S.C. § 2511(2)(f) (West Supp. 2005) (carving out from statutory regulation only the acquisition of intelligence information from "international or foreign communications" and

“foreign intelligence activities . . . involving a foreign electronic communications system” as long as they are accomplished “utilizing a means other than electronic surveillance as defined in section 101” of FISA). Congress also defined “electronic surveillance,” 50 U.S.C. § 1801(f), carefully and somewhat narrowly.⁶

In addition, Congress addressed, to some degree, the manner in which FISA might apply after a formal declaration of war by expressly allowing warrantless surveillance for a period of fifteen days following such a declaration. Section 111 of FISA allows the President to “authorize electronic surveillance without a court order under this subchapter to acquire foreign intelligence information for a period not to exceed fifteen calendar days following a declaration of war by the Congress.” 50 U.S.C. § 1811.

The legislative history of FISA shows that Congress understood it was legislating on fragile constitutional ground and was pressing or even exceeding constitutional limits in regulating the President’s authority in the field of foreign intelligence. The final House Conference Report, for example, recognized that the statute’s restrictions might well impermissibly infringe on the President’s constitutional powers. That report includes the extraordinary acknowledgment that “[t]he conferees agree that the establishment by this act of exclusive means by which the President may conduct electronic surveillance does not foreclose a different decision by the Supreme Court.” H.R. Conf. Rep. No. 95-1720, at 35, *reprinted in* 1978 U.S.C.C.A.N. 4048, 4064. But, invoking Justice Jackson’s concurrence in the *Steel Seizure* case, the Conference Report explained that Congress intended in FISA to exert whatever power Congress constitutionally had over the subject matter to restrict foreign intelligence surveillance and to leave the President solely with whatever inherent constitutional authority he might be able to invoke against Congress’s express wishes. *Id.* The Report thus explains that “[t]he intent of the conferees is to apply the standard set forth in Justice Jackson’s concurring opinion in the *Steel Seizure* Case: ‘When a President takes measures incompatible with the express or implied

⁶ FISA’s legislative history reveals that these provisions were intended to exclude certain intelligence activities conducted by the National Security Agency from the coverage of FISA. According to the report of the Senate Judiciary Committee on FISA, “this provision [referencing what became the first part of section 2511(2)(f)] is designed to make clear that the legislation does not deal with international signals intelligence activities as currently engaged in by the National Security Agency and electronic surveillance conducted outside the United States.” S. Rep. No. 95-604, at 64 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3904, 3965. The legislative history also makes clear that the definition of “electronic surveillance” was crafted for the same reason. *See id.* at 33-34, 1978 U.S.C.C.A.N. at 3934-36. FISA thereby “adopts the view expressed by the Attorney General during the hearings that enacting statutory controls to regulate the National Security Agency and the surveillance of Americans abroad raises problems best left to separate legislation.” *Id.* at 64, 1978 U.S.C.C.A.N. at 3965. Such legislation placing limitations on traditional NSA activities was drafted, but never passed. *See* National Intelligence Reorganization and Reform Act of 1978: Hearings Before the Senate Select Committee on Intelligence, 95th Cong., 2d Sess. 999-1007 (1978) (text of unenacted legislation). And Congress understood that the NSA surveillance that it intended categorically to exclude from FISA could include the monitoring of international communications into or out of the United States of U.S. citizens. The report specifically referred to the Church Committee report for its description of the NSA’s activities, S. Rep. No. 95-604, at 64 n.63, 1978 U.S.C.C.A.N. at 3965-66 n.63, which stated that “the NSA intercepts messages passing over international lines of communication, some of which have one terminal within the United States. Traveling over these lines of communication, especially those with one terminal in the United States, are messages of Americans” S. Rep. 94-755, at Book II, 308 (1976). Congress’s understanding in the legislative history of FISA that such communications could be intercepted outside FISA procedures is notable.

will of Congress, his power is at the lowest ebb, for then he can rely only upon his own constitutional power minus any constitutional power of Congress over the matter.” *Id.* (quoting *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 637 (1952) (Jackson, J., concurring)); see also S. Rep. No. 95-604, at 64, reprinted in 1978 U.S.C.C.A.N. at 3966 (same); see generally Elizabeth B. Bazen et al., Congressional Research Service, *Re: Presidential Authority to Conduct Warrantless Electronic Surveillance to Gather Foreign Intelligence Information* 28-29 (Jan. 5, 2006). It is significant, however, that Congress did not decide conclusively to continue to push the boundaries of its constitutional authority in wartime. Instead, Congress reserved the question of the appropriate procedures to regulate electronic surveillance in time of war, and established a fifteen-day period during which the President would be permitted to engage in electronic surveillance without complying with FISA’s express procedures and during which Congress would have the opportunity to revisit the issue. See 50 U.S.C. § 1811; H.R. Conf. Rep. No. 95-1720, at 34, reprinted in 1978 U.S.C.C.A.N. at 4063 (noting that the purpose of the fifteen-day period following a declaration of war in section 111 of FISA was to “allow time for consideration of any amendment to this act that may be appropriate during a wartime emergency”).

B. FISA CONTEMPLATES AND ALLOWS SURVEILLANCE AUTHORIZED “BY STATUTE”

Congress did not attempt through FISA to prohibit the Executive Branch from using electronic surveillance. Instead, Congress acted to bring the exercise of that power under more stringent congressional control. See, e.g., H. Conf. Rep. No. 95-1720, at 32, reprinted in 1978 U.S.C.C.A.N. 4048, 4064. Congress therefore enacted a regime intended to supplant the President’s reliance on his own constitutional authority. Consistent with this overriding purpose of bringing the use of electronic surveillance under congressional control and with the commonsense notion that the Congress that enacted FISA could not bind future Congresses, FISA expressly contemplates that the Executive Branch may conduct electronic surveillance outside FISA’s express procedures if and when a subsequent statute authorizes such surveillance.

Thus, section 109 of FISA prohibits any person from intentionally “engag[ing] . . . in electronic surveillance under color of law *except as authorized by statute.*” 50 U.S.C. § 1809(a)(1) (emphasis added). Because FISA’s prohibitory provision broadly exempts surveillance “authorized by statute,” the provision demonstrates that Congress did not attempt to regulate through FISA electronic surveillance authorized by Congress through a subsequent enactment. The use of the term “statute” here is significant because it strongly suggests that any subsequent authorizing statute, not merely one that amends FISA itself, could legitimately authorize surveillance outside FISA’s standard procedural requirements. Compare 18 U.S.C. § 2511(1) (“Except as otherwise specifically provided *in this chapter* any person who—(a) intentionally intercepts . . . any wire, oral, or electronic communication[] . . . shall be punished . . .”) (emphasis added); *id.* § 2511(2)(e) (providing a defense to liability to individuals “conduct[ing] electronic surveillance, . . . as authorized by *that Act [FISA]*”) (emphasis added). In enacting FISA, therefore, Congress contemplated the possibility that the President might be permitted to conduct electronic surveillance pursuant to a later-enacted statute that did not

incorporate all of the procedural requirements set forth in FISA or that did not expressly amend FISA itself.

To be sure, the scope of this exception is rendered less clear by the conforming amendments that FISA made to chapter 119 of title 18—the portion of the criminal code that provides the mechanism for obtaining wiretaps for law enforcement purposes. Before FISA was enacted, chapter 119 made it a criminal offense for any person to intercept a communication except as specifically provided in that chapter. See 18 U.S.C. § 2511(1)(a), (4)(a). Section 201(b) of FISA amended that chapter to provide an exception from criminal liability for activities conducted pursuant to FISA. Specifically, FISA added 18 U.S.C. § 2511(2)(e), which provides that it is not unlawful for “an officer, employee, or agent of the United States . . . to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, as authorized by that Act.” *Id.* § 2511(2)(e). Similarly, section 201(b) of FISA amended chapter 119 to provide that “procedures in this chapter [or chapter 121 (addressing access to stored wire and electronic communications and customer records)] and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance, as defined in section 101 of such Act, and the interception of domestic wire, oral, and electronic communications may be conducted.” *Id.* § 2511(2)(f) (West Supp. 2005).⁷

The amendments that section 201(b) of FISA made to title 18 are fully consistent, however, with the conclusion that FISA contemplates that a subsequent statute could authorize electronic surveillance outside FISA’s express procedural requirements. Section 2511(2)(e) of title 18, which provides that it is “not unlawful” for an officer of the United States to conduct electronic surveillance “as authorized by” FISA, is best understood as a safe-harbor provision. Because of section 109, the protection offered by section 2511(2)(e) for surveillance “authorized by” FISA extends to surveillance that is authorized by any other statute and therefore excepted from the prohibition of section 109. In any event, the purpose of section 2511(2)(e) is merely to make explicit what would already have been implicit—that those authorized by statute to engage in particular surveillance do not act unlawfully when they conduct such surveillance. Thus, even if that provision had not been enacted, an officer conducting surveillance authorized by statute (whether FISA or some other law) could not reasonably have been thought to be violating Title III. Similarly, section 2511(2)(e) cannot be read to require a result that would be manifestly unreasonable—exposing a federal officer to criminal liability for engaging in surveillance authorized by statute, merely because the authorizing statute happens not to be FISA itself.

Nor could 18 U.S.C. § 2511(2)(f), which provides that the “procedures in this chapter . . . and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance . . . may be conducted,” have been intended to trump the commonsense approach of section 109 and preclude a subsequent Congress from authorizing the President to engage in electronic surveillance through a statute other than FISA, using procedures other than those outlined in FISA or chapter 119 of title 18. The legislative history of section 2511(2)(f) clearly indicates an intent to prevent the President from engaging in surveillance except as

⁷ The bracketed portion was added in 1986 amendments to section 2511(2)(f). See Pub. L. No. 99-508 § 101(b)(3), 100 Stat. 1848, 1850.

authorized by Congress, *see* H.R. Conf. Rep. No. 95-1720, at 32, *reprinted in* 1978 U.S.C.C.A.N. 4048, 4064, which explains why section 2511(2)(f) set forth all then-existing statutory restrictions on electronic surveillance. Section 2511(2)(f)'s reference to "exclusive means" reflected the state of statutory authority for electronic surveillance in 1978 and cautioned the President not to engage in electronic surveillance outside congressionally sanctioned parameters. It is implausible to think that, in attempting to limit the *President's* authority, Congress also limited its own future authority by barring subsequent Congresses from authorizing the Executive to engage in surveillance in ways not specifically enumerated in FISA or chapter 119, or by requiring a subsequent Congress specifically to amend FISA and section 2511(2)(f). There would be a serious question as to whether the Ninety-Fifth Congress could have so tied the hands of its successors. *See, e.g., Fletcher v. Peck*, 10 U.S. (6 Cranch) 87, 135 (1810) (noting that "one legislature cannot abridge the powers of a succeeding legislature"); *Reichelderfer v. Quinn*, 287 U.S. 315, 318 (1932) ("[T]he will of a particular Congress . . . does not impose itself upon those to follow in succeeding years"); *Lockhart v. United States*, 126 S. Ct. 699, 703 (2005) (Scalia, J., concurring) (collecting precedent); 1 W. Blackstone, *Commentaries on the Laws of England* 90 (1765) ("Acts of parliament derogatory from the power of subsequent parliaments bind not"). In the absence of a clear statement to the contrary, it cannot be presumed that Congress attempted to abnegate its own authority in such a way.

Far from a clear statement of congressional intent to bind itself, there are indications that section 2511(2)(f) cannot be interpreted as requiring that *all* electronic surveillance and domestic interception be conducted under FISA's enumerated procedures or those of chapter 119 of title 18 until and unless those provisions are repealed or amended. Even when section 2511(2)(f) was enacted (and no subsequent authorizing statute existed), it could not reasonably be read to preclude all electronic surveillance conducted outside the procedures of FISA or chapter 119 of title 18. In 1978, use of a pen register or trap and trace device constituted electronic surveillance as defined by FISA. *See* 50 U.S.C. §§ 1801(f), (n). Title I of FISA provided procedures for obtaining court authorization for the use of pen registers to obtain foreign intelligence information. But the Supreme Court had, just prior to the enactment of FISA, held that chapter 119 of title 18 did not govern the use of pen registers. *See United States v. New York Tel. Co.*, 434 U.S. 159, 165-68 (1977). Thus, if section 2511(2)(f) were to be read to permit of no exceptions, the use of pen registers for purposes other than to collect foreign intelligence information would have been unlawful because such use would not have been authorized by the "exclusive" procedures of section 2511(2)(f), *i.e.*, FISA and chapter 119. But no court has held that pen registers could not be authorized outside the foreign intelligence context. Indeed, FISA appears to have recognized this issue by providing a defense to liability for any official who engages in electronic surveillance under a search warrant or court order. *See* 50 U.S.C. § 1809(b). (The practice when FISA was enacted was for law enforcement officers to obtain search warrants under the Federal Rules of Criminal Procedure authorizing the installation and use of pen registers. *See S. 1667, A Bill to Amend Title 18, United States Code, with Respect to the Interception of Certain Communications, Other Forms of Surveillance, and for Other Purposes: Hearing Before the Subcomm. On Patents, Copyrights and Trademarks of the Senate*

*Comm. on the Judiciary, 99th Cong. 57 (1985) (prepared statement of James Knapp, Deputy Assistant Attorney General, Criminal Division)).*⁸

In addition, section 2511(2)(a)(ii) authorizes telecommunications providers to assist officers of the Government engaged in electronic surveillance when the Attorney General certifies that "no warrant or court order is required by law [and] that all statutory requirements have been met." 18 U.S.C. § 2511(2)(a)(ii).⁹ If the Attorney General can certify, in good faith, that the requirements of a subsequent statute authorizing electronic surveillance are met, service providers are affirmatively and expressly authorized to assist the Government. Although FISA does allow the Government to proceed without a court order in several situations, *see* 50 U.S.C. § 1805(f) (emergencies); *id.* § 1802 (certain communications between foreign governments), this provision specifically lists only Title III's emergency provision but speaks generally to Attorney General certification. That reference to Attorney General certification is consistent with the historical practice in which Presidents have delegated to the Attorney General authority to approve warrantless surveillance for foreign intelligence purposes. *See, e.g., United States v. United States District Court*, 444 F.2d 651, 669-71 (6th Cir. 1971) (reproducing as an appendix memoranda from Presidents Roosevelt, Truman, and Johnson). Section 2511(2)(a)(ii) thus suggests that telecommunications providers can be authorized to assist with warrantless electronic surveillance when such surveillance is authorized by law outside FISA.

In sum, by expressly and broadly excepting from its prohibition electronic surveillance undertaken "as authorized by statute," section 109 of FISA permits an exception to the "procedures" of FISA referred to in 18 U.S.C. § 2511(2)(f) where authorized by another statute, even if the other authorizing statute does not specifically amend section 2511(2)(f).

C. THE AUMF IS A "STATUTE" AUTHORIZING SURVEILLANCE OUTSIDE THE CONFINES OF FISA

The AUMF qualifies as a "statute" authorizing electronic surveillance within the meaning of section 109 of FISA.

First, because the term "statute" historically has been given broad meaning, the phrase "authorized by statute" in section 109 of FISA must be read to include joint resolutions such as

⁸ Alternatively, section 109(b) may be read to constitute a "procedure" in FISA or to incorporate procedures from sources other than FISA (such as the Federal Rules of Criminal Procedure or state court procedures), and in that way to satisfy section 2511(2)(f). But if section 109(b)'s defense can be so read, section 109(a) should also be read to constitute a procedure or incorporate procedures not expressly enumerated in FISA.

⁹ Section 2511(2)(a)(ii) states:

Notwithstanding any other law, providers of wire or electronic communication service, . . . are authorized by law to provide information, facilities, or technical assistance to persons authorized by law to intercept . . . communications or to conduct electronic surveillance, as defined [by FISA], if such provider . . . has been provided with . . . a certification in writing by [specified persons proceeding under Title III's emergency provision] or the Attorney General of the United States that no warrant or court order is required by law, that all statutory requirements have been met, and that the specific assistance is required.

the AUMF. *See American Fed'n of Labor v. Watson*, 327 U. S. 582, 592-93 (1946) (finding the term "statute" as used in 28 U.S.C. § 380 to mean "a compendious summary of various enactments, by whatever method they may be adopted, to which a State gives her sanction"); Black's Law Dictionary 1410 (6th ed. 1990) (defining "statute" broadly to include any "formal written enactment of a legislative body," and stating that the term is used "to designate the legislatively created laws in contradistinction to court decided or unwritten laws"). It is thus of no significance to this analysis that the AUMF was enacted as a joint resolution rather than a bill. *See, e.g., Ann Arbor R.R. Co. v. United States*, 281 U.S. 658, 666 (1930) (joint resolutions are to be construed by applying "the rules applicable to legislation in general"); *United States ex rel. Levey v. Stockslager*, 129 U.S. 470, 475 (1889) (joint resolution had "all the characteristics and effects" of statute that it suspended); *Padilla ex rel. Newman v. Bush*, 233 F. Supp. 2d 564, 598 (S.D.N.Y. 2002) (in analyzing the AUMF, finding that there is "no relevant constitutional difference between a bill and a joint resolution"), *rev'd sub. nom. on other grounds, Rumsfeld v. Padilla*, 352 F.3d 695 (2d Cir. 2003), *rev'd*, 542 U.S. 426 (2004); *see also* Letter for the Hon. John Conyers, Jr., U.S. House of Representatives, from Prof. Laurence H. Tribe at 3 (Jan. 6, 2006) (term "statute" in section 109 of FISA "of course encompasses a joint resolution presented to and signed by the President").

Second, the longstanding history of communications intelligence as a fundamental incident of the use of force and the Supreme Court's decision in *Hamdi v. Rumsfeld* strongly suggest that the AUMF satisfies the requirement of section 109 of FISA for statutory authorization of electronic surveillance. As explained above, it is not necessary to demarcate the outer limits of the AUMF to conclude that it encompasses electronic surveillance targeted at the enemy. Just as a majority of the Court concluded in *Hamdi* that the AUMF authorizes detention of U.S. citizens who are enemy combatants without expressly mentioning the President's long-recognized power to detain, so too does it authorize the use of electronic surveillance without specifically mentioning the President's equally long-recognized power to engage in communications intelligence targeted at the enemy. And just as the AUMF satisfies the requirement in 18 U.S.C. § 4001(a) that no U.S. citizen be detained "except pursuant to an Act of Congress," so too does it satisfy section 109's requirement for statutory authorization of electronic surveillance.¹⁰ In authorizing the President's use of force in response to the September 11th attacks, Congress did not need to comb through the United States Code looking for those restrictions that it had placed on national security operations during times of peace and designate with specificity each traditional tool of military force that it sought to authorize the President to use. There is no historical precedent for such a requirement: authorizations to use

¹⁰ It might be argued that Congress dealt more comprehensively with electronic surveillance in FISA than it did with detention in 18 U.S.C. § 4001(a). Thus, although Congress prohibited detention "except pursuant to an Act of Congress," it combined the analogous prohibition in FISA (section 109(a)) with section 2511(2)(f)'s exclusivity provision. *See* Letter to the Hon. Bill Frist, Majority Leader, U.S. Senate, from Professor Curtis A. Bradley *et al.* at 5 n.6 (Jan. 9, 2006) (noting that section 4001(a) does not "attempt[] to create an exclusive mechanism for detention"). On closer examination, however, it is evident that Congress has regulated detention far more meticulously than these arguments suggest. Detention is the topic of much of the Criminal Code, as well as a variety of other statutes, including those providing for civil commitment of the mentally ill and confinement of alien terrorists. The existence of these statutes and accompanying extensive procedural safeguards, combined with the substantial constitutional issues inherent in detention, *see, e.g., Hamdi*, 542 U.S. at 574-75 (Scalia, J., dissenting), refute any such argument.

military force traditionally have been couched in general language. Indeed, prior administrations have interpreted joint resolutions declaring war and authorizing the use of military force to authorize expansive collection of communications into and out of the United States.¹¹

Moreover, crucial to the Framers' decision to vest the President with primary constitutional authority to defend the Nation from foreign attack is the fact that the Executive can act quickly, decisively, and flexibly as needed. For Congress to have a role in that process, it must be able to act with similar speed, either to lend its support to, or to signal its disagreement with, proposed military action. Yet the need for prompt decisionmaking in the wake of a devastating attack on the United States is fundamentally inconsistent with the notion that to do so Congress must legislate at a level of detail more in keeping with a peacetime budget reconciliation bill. In emergency situations, Congress must be able to use broad language that effectively sanctions the President's use of the core incidents of military force. That is precisely what Congress did when it passed the AUMF on September 14, 2001—just three days after the deadly attacks on America. The Capitol had been evacuated on September 11th, and Congress was meeting in scattered locations. As an account emerged of who might be responsible for these attacks, Congress acted quickly to authorize the President to use "all necessary and appropriate force" against the enemy that he determines was involved in the September 11th attacks. Under these circumstances, it would be unreasonable and wholly impractical to demand that Congress specifically amend FISA in order to assist the President in defending the Nation. Such specificity would also have been self-defeating because it would have apprised our adversaries of some of our most sensitive methods of intelligence gathering.¹²

Section 111 of FISA, 50 U.S.C. § 1811, which authorizes the President, "[n]otwithstanding any other law," to conduct "electronic surveillance without a court order under this subchapter to acquire foreign intelligence information for a period not to exceed fifteen calendar days following a declaration of war by Congress," does not require a different reading of the AUMF. *See also id.* § 1844 (same provision for pen registers); *id.* § 1829 (same provision for physical searches). Section 111 cannot reasonably be read as Congress's final word on electronic surveillance during wartime, thus permanently limiting the President in all

¹¹ As noted above, in intercepting communications, President Wilson relied on his constitutional authority and the joint resolution declaring war and authorizing the use of military force, which, as relevant here, provided "that the President [is] authorized and directed to employ the entire naval and military forces of the United States and the resources of the Government to carry on war against the Imperial German Government; and to bring the conflict to a successful termination all of the resources of the country are hereby pledged by the Congress of the United States." Joint Resolution of Apr. 6, 1917, ch. 1, 40 Stat. 1. The authorization did not explicitly mention interception of communications.

¹² Some have suggested that the Administration declined to seek a specific amendment to FISA allowing the NSA activities "because it was advised that Congress would reject such an amendment," Letter to the Hon. Bill Frist, Majority Leader, U.S. Senate, from Professor Curtis A. Bradley *et al.* 4 & n.4 (Jan. 9, 2005), and they have quoted in support of that assertion the Attorney General's statement that certain Members of Congress advised the Administration that legislative relief "would be difficult, if not impossible." *Id.* at 4 n.4. As the Attorney General subsequently indicated, however, the difficulty with such specific legislation was that it could not be enacted "without compromising the program." *See* Remarks by Homeland Security Secretary Chertoff and Attorney General Gonzales on the USA PATRIOT Act (Dec. 21, 2005), available at <http://www.dhs.gov/dhspublic/display?content=5285>.

circumstances to a mere fifteen days of warrantless military intelligence gathering targeted at the enemy following a declaration of war. Rather, section 111 represents Congress's recognition that it would likely have to return to the subject and provide additional authorization to conduct warrantless electronic surveillance outside FISA during time of war. The Conference Report explicitly stated the conferees' "inten[t] that this [fifteen-day] period will allow time for consideration of any amendment to this act that may be appropriate during a wartime emergency." H.R. Conf. Rep. No. 95-1720, at 34, *reprinted in* 1978 U.S.C.C.A.N. at 4063. Congress enacted section 111 so that the President could conduct warrantless surveillance while Congress considered supplemental wartime legislation.

Nothing in the terms of section 111 disables Congress from authorizing such electronic surveillance as a traditional incident of war through a broad, conflict-specific authorization for the use of military force, such as the AUMF. Although the legislative history of section 111 indicates that in 1978 some Members of Congress believed that any such authorization would come in the form of a particularized amendment to FISA itself, section 111 does not require that result. Nor could the Ninety-Fifth Congress tie the hands of a subsequent Congress in this way, at least in the absence of far clearer statutory language expressly requiring that result. *See supra*, pp. 21-22; *compare, e.g.*, War Powers Resolution, § 8, 50 U.S.C. § 1547(a) ("Authority to introduce United States Armed Forces into hostilities . . . shall not be inferred . . . from any provision of law . . . unless such provision specifically authorizes [such] introduction . . . and states that it is intended to constitute specific statutory authorization within the meaning of this chapter."); 10 U.S.C. § 401 (stating that any other provision of law providing assistance to foreign countries to detect and clear landmines shall be subject to specific limitations and may be construed as superseding such limitations "only if, and to the extent that, such provision specifically refers to this section and specifically identifies the provision of this section that is to be considered superseded or otherwise inapplicable"). An interpretation of section 111 that would disable Congress from authorizing broader electronic surveillance in that form can be reconciled neither with the purposes of section 111 nor with the well-established proposition that "one legislature cannot abridge the powers of a succeeding legislature." *Fletcher v. Peck*, 10 U.S. (6 Cranch) at 135; *see supra* Part II.B. For these reasons, the better interpretation is that section 111 was not intended to, and did not, foreclose Congress from using the AUMF as the legal vehicle for supplementing the President's existing authority under FISA in the battle against al Qaeda.

The contrary interpretation of section 111 also ignores the important differences between a formal declaration of war and a resolution such as the AUMF. As a historical matter, a formal declaration of war was no longer than a sentence, and thus Congress would not expect a declaration of war to outline the extent to which Congress authorized the President to engage in various incidents of waging war. Authorizations for the use of military force, by contrast, are typically more detailed and are made for the *specific purpose* of reciting the manner in which Congress has authorized the President to act. Thus, Congress could reasonably expect that an authorization for the use of military force would address the issue of wartime surveillance, while a declaration of war would not. Here, the AUMF declares that the Nation faces "an unusual and extraordinary threat," acknowledges that "the President has authority under the Constitution to take action to deter and prevent acts of international terrorism against the United States," and

provides that the President is authorized "to use all necessary and appropriate force" against those "he determines" are linked to the September 11th attacks. AUMF pmb., § 2. This sweeping language goes far beyond the bare terms of a declaration of war. *Compare, e.g.,* Act of Apr. 25, 1898, ch. 189, 30 Stat. 364 ("First. That war be, and the same is hereby declared to exist . . . between the United States of America and the Kingdom of Spain.").

Although legislation that has included a declaration of war has often also included an authorization of the President to use force, these provisions are separate and need not be combined in a single statute. *See, e.g., id.* ("Second. That the President of the United States be, and he hereby is, directed and empowered to use the entire land and naval forces of the United States, and to call into the actual service of the United States the militia of the several states, *to such extent as may be necessary to carry this Act into effect.*") (emphasis added). Moreover, declarations of war have legal significance independent of any additional authorization of force that might follow. *See, e.g.,* Louis Henkin, *Foreign Affairs and the U.S. Constitution* 75 (2d ed. 1996) (explaining that a formal state of war has various legal effects, such as terminating diplomatic relations, and abrogating or suspending treaty obligations and international law rights and duties); *see also id.* at 370 n.65 (speculating that one reason to fight an undeclared war would be to "avoid the traditional consequences of declared war on relations with third nations or even . . . belligerents").

In addition, section 111 does not cover the vast majority of modern military conflicts. The last declared war was World War II. Indeed, the most recent conflict prior to the passage of FISA, Vietnam, was fought without a formal declaration of war. In addition, the War Powers Resolution, enacted less than five years before FISA, clearly recognizes the distinctions between formal declarations of war and authorizations of force and demonstrates that, if Congress had wanted to include such authorizations in section 111, it knew how to do so. *See, e.g.,* 50 U.S.C. § 1544(b) (attempting to impose certain consequences 60 days after reporting the initiation of hostilities to Congress "unless the Congress . . . has declared war *or has enacted a specific authorization for such use*" of military force) (emphasis added). It is possible that, in enacting section 111, Congress intended to make no provision for even the temporary use of electronic surveillance without a court order for what had become the legal regime for most military conflicts. A better reading, however, is that Congress assumed that such a default provision would be unnecessary because, if it had acted through an authorization for the use of military force, the more detailed provisions of that authorization would resolve the extent to which Congress would attempt to authorize, or withhold authorization for, the use of electronic surveillance.¹³

¹³ Some have pointed to the specific amendments to FISA that Congress made shortly after September 11th in the USA PATRIOT Act, Pub. L. No. 107-56, §§ 204, 218, 115 Stat. 272, 281, 291 (2001), to argue that Congress did not contemplate electronic surveillance outside the parameters of FISA. *See Memorandum for Members of the House Permanent Select Comm. on Intel. from Jeffrey H. Smith, Re: Legal Authorities Regarding Warrantless Surveillance of U.S. Persons* 6-7 (Jan. 3, 2006). The USA PATRIOT Act amendments, however, do not justify giving the AUMF an unnaturally narrow reading. The USA PATRIOT Act amendments made important corrections in the general application of FISA; they were not intended to define the precise incidents of military force that would be available to the President in prosecuting the current armed conflict against al Qaeda and its allies. Many removed long-standing impediments to the effectiveness of FISA that had contributed to the

* * *

The broad text of the AUMF, the authoritative interpretation that the Supreme Court gave it in *Hamdi*, and the circumstances in which it was passed demonstrate that the AUMF is a statute authorizing electronic surveillance under section 109 of FISA. When the President authorizes electronic surveillance against the enemy pursuant to the AUMF, he is therefore acting at the height of his authority under *Youngstown*, 343 U.S. at 637 (Jackson, J., concurring).

D. THE CANON OF CONSTITUTIONAL AVOIDANCE REQUIRES RESOLVING IN FAVOR OF THE PRESIDENT'S AUTHORITY ANY AMBIGUITY ABOUT WHETHER FISA FORBIDS THE NSA ACTIVITIES

As explained above, the AUMF fully authorizes the NSA activities. Because FISA contemplates the possibility that subsequent statutes could authorize electronic surveillance without requiring FISA's standard procedures, the NSA activities are also consistent with FISA and related provisions in title 18. Nevertheless, some might argue that sections 109 and 111 of FISA, along with section 2511(2)(f)'s "exclusivity" provision and section 2511(2)(e)'s liability exception for officers engaged in FISA-authorized surveillance, are best read to suggest that FISA requires that subsequent authorizing legislation specifically amend FISA in order to free the Executive from FISA's enumerated procedures. As detailed above, this is not the better reading of FISA. But even if these provisions were ambiguous, any doubt as to whether the AUMF and FISA should be understood to allow the President to make tactical military decisions to authorize surveillance outside the parameters of FISA must be resolved to avoid the serious constitutional questions that a contrary interpretation would raise.

It is well established that the first task of any interpreter faced with a statute that may present an unconstitutional infringement on the powers of the President is to determine whether the statute may be construed to avoid the constitutional difficulty. "[I]f an otherwise acceptable

maintenance of an unnecessary "wall" between foreign intelligence gathering and criminal law enforcement; others were technical clarifications. See *In re Sealed Case*, 310 F.3d 717, 725-30 (Foreign Int. Surv. Ct. Rev. 2002). The "wall" had been identified as a significant problem hampering the Government's efficient use of foreign intelligence information well before the September 11th attacks and in contexts unrelated to terrorism. See, e.g., *Final Report of the Attorney General's Review Team on the Handling of the Los Alamos National Laboratory Investigation* 710, 729, 732 (May 2000); General Accounting Office, *FBI Intelligence Investigations: Coordination Within Justice on Counterintelligence Criminal Matters Is Limited* (GAO-01-780) 3, 31 (July 2001). Finally, it is worth noting that Justice Souter made a similar argument in *Hamdi* that the USA PATRIOT Act all but compelled a narrow reading of the AUMF. See 542 U.S. at 551 ("It is very difficult to believe that the same Congress that carefully circumscribed Executive power over alien terrorists on home soil [in the USA PATRIOT Act] would not have meant to require the Government to justify clearly its detention of an American citizen held on home soil incommunicado."). Only Justice Ginsburg joined this opinion, and the position was rejected by a majority of Justices.

Nor do later amendments to FISA undermine the conclusion that the AUMF authorizes electronic surveillance outside the procedures of FISA. Three months after the enactment of the AUMF, Congress enacted certain "technical amendments" to FISA which, *inter alia*, extended the time during which the Attorney General may issue an emergency authorization of electronic surveillance from 24 to 72 hours. See Intelligence Authorization Act for Fiscal Year 2002, Pub. L. No. 107-108, § 314, 115 Stat. 1394, 1402 (2001). These modifications to FISA do not in any way undermine Congress's previous authorization in the AUMF for the President to engage in electronic surveillance outside the parameters of FISA in the specific context of the armed conflict with al Qaeda.

construction of a statute would raise serious constitutional problems, and where an alternative interpretation of the statute is 'fairly possible,' we are obligated to construe the statute to avoid such problems." *INS v. St. Cyr*, 533 U.S. 289, 299-300 (2001) (citations omitted); *Ashwander v. TVA*, 297 U.S. 288, 345-48 (1936) (Brandeis, J., concurring). Moreover, the canon of constitutional avoidance has particular importance in the realm of national security, where the President's constitutional authority is at its highest. See *Department of the Navy v. Egan*, 484 U.S. 518, 527, 530 (1988); William N. Eskridge, Jr., *Dynamic Statutory Interpretation* 325 (1994) (describing "[s]uper-strong rule against congressional interference with the President's authority over foreign affairs and national security"). Thus, courts and the Executive Branch typically construe a general statute, even one that is written in unqualified terms, to be implicitly limited so as not to infringe on the President's Commander in Chief powers.

Reading FISA to prohibit the NSA activities would raise two serious constitutional questions, both of which must be avoided if possible: (1) whether the signals intelligence collection the President determined was necessary to undertake is such a core exercise of Commander in Chief control over the Armed Forces during armed conflict that Congress cannot interfere with it at all and (2) whether the particular restrictions imposed by FISA are such that their application would impermissibly impede the President's exercise of his constitutionally assigned duties as Commander in Chief. Constitutional avoidance principles require interpreting FISA, at least in the context of the military conflict authorized by the AUMF, to avoid these questions, if "fairly possible." Even if Congress intended FISA to use the full extent of its constitutional authority to "occupy the field" of "electronic surveillance," as FISA used that term, during peacetime, the legislative history indicates that Congress had not reached a definitive conclusion about its regulation during wartime. See H.R. Conf. Rep. No. 95-1720, at 34, reprinted in 1978 U.S.C.C.A.N. at 4063 (noting that the purpose of the fifteen-day period following a declaration of war in section 111 of FISA was to "allow time for consideration of any amendment to this act that may be appropriate during a wartime emergency"). Therefore, it is not clear that Congress, in fact, intended to test the limits of its constitutional authority in the context of wartime electronic surveillance.

Whether Congress may interfere with the President's constitutional authority to collect foreign intelligence information through interception of communications reasonably believed to be linked to the enemy poses a difficult constitutional question. As explained in Part I, it had long been accepted at the time of FISA's enactment that the President has inherent constitutional authority to conduct warrantless electronic surveillance for foreign intelligence purposes. Congress recognized at the time that the enactment of a statute purporting to eliminate the President's ability, even during peacetime, to conduct warrantless electronic surveillance to collect foreign intelligence was near or perhaps beyond the limit of Congress's Article I powers. The NSA activities, however, involve signals intelligence performed in the midst of a congressionally authorized armed conflict undertaken to prevent further hostile attacks on the United States. The NSA activities lie at the very core of the Commander in Chief power, especially in light of the AUMF's explicit authorization for the President to take *all* necessary and appropriate military action to stop al Qaeda from striking again. The constitutional principles at stake here thus involve not merely the President's well-established inherent

authority to conduct warrantless surveillance for foreign intelligence purposes during peacetime, but also the powers and duties expressly conferred on him as Commander in Chief by Article II.

Even outside the context of wartime surveillance of the enemy, the source and scope of Congress's power to restrict the President's inherent authority to conduct foreign intelligence surveillance is unclear. As explained above, the President's role as sole organ for the Nation in foreign affairs has long been recognized as carrying with it preeminent authority in the field of national security and foreign intelligence. The source of this authority traces to the Vesting Clause of Article II, which states that "[t]he executive Power shall be vested in a President of the United States of America." U.S. Const. art. II, § 1. The Vesting Clause "has long been held to confer on the President plenary authority to represent the United States and to pursue its interests outside the borders of the country, subject only to limits specifically set forth in the Constitution itself and to such statutory limitations as the Constitution permits Congress to impose by exercising one of its enumerated powers." *The President's Compliance with the "Timely Notification" Requirement of Section 501(b) of the National Security Act*, 10 Op. O.L.C. 159, 160-61 (1986) ("*Timely Notification Requirement Op.*").

Moreover, it is clear that some presidential authorities in this context are beyond Congress's ability to regulate. For example, as the Supreme Court explained in *Curtiss-Wright*, the President "*makes treaties with the advice and consent of the Senate; but he alone negotiates. Into the field of negotiation the Senate cannot intrude; and Congress itself is powerless to invade it.*" 299 U.S. at 319. Similarly, President Washington established early in the history of the Republic the Executive's absolute authority to maintain the secrecy of negotiations with foreign powers, even against congressional efforts to secure information. *See id.* at 320-21. Recognizing presidential authority in this field, the Executive Branch has taken the position that "congressional legislation authorizing extraterritorial diplomatic and intelligence activities is superfluous, and . . . statutes infringing the President's inherent Article II authority would be unconstitutional." *Timely Notification Requirement Op.*, 10 Op. O.L.C. at 164.

There are certainly constitutional limits on Congress's ability to interfere with the President's power to conduct foreign intelligence searches, consistent with the Constitution, within the United States. As explained above, intelligence gathering is at the heart of executive functions. Since the time of the Founding it has been recognized that matters requiring secrecy—and intelligence in particular—are quintessentially executive functions. *See, e.g., The Federalist No. 64*, at 435 (John Jay) (Jacob E. Cooke ed. 1961) ("The convention have done well therefore in so disposing of the power of making treaties, that although the president must in forming them act by the advice and consent of the senate, yet he will be able to manage the business of intelligence in such manner as prudence may suggest."); *see also Timely Notification Requirement Op.*, 10 Op. O.L.C. at 165; *cf. New York Times Co. v. United States*, 403 U.S. 713, 729-30 (1971) (Stewart, J., concurring) ("[I]t is the constitutional duty of the Executive—as a matter of sovereign prerogative and not as a matter of law as the courts know law—through the promulgation and enforcement of executive regulations, to protect the confidentiality necessary to carry out its responsibilities in the field of international relations and national defense.").

Because Congress has rarely attempted to intrude in this area and because many of these questions are not susceptible to judicial review, there are few guideposts for determining exactly where the line defining the President's sphere of exclusive authority lies. Typically, if a statute is in danger of encroaching upon exclusive powers of the President, the courts apply the constitutional avoidance canon, if a construction avoiding the constitutional issue is "fairly possible." *See, e.g., Egan*, 484 U.S. at 527, 530. The only court that squarely has addressed the relative powers of Congress and the President in this field suggested that the balance tips decidedly in the President's favor. The Foreign Intelligence Surveillance Court of Review recently noted that all courts to have addressed the issue of the President's inherent authority have "held that the President did have inherent authority to conduct warrantless searches to obtain foreign intelligence information." *In re Sealed Case*, 310 F.3d 717, 742 (Foreign Intel. Surv. Ct. of Rev. 2002). On the basis of that unbroken line of precedent, the court "[took] for granted that the President does have that authority," and concluded that, "assuming that is so, FISA could not encroach on the President's constitutional power." *Id.*¹⁴ Although the court did not provide extensive analysis, it is the only judicial statement on point, and it comes from the specialized appellate court created expressly to deal with foreign intelligence issues under FISA.

But the NSA activities are not simply exercises of the President's general foreign affairs powers. Rather, they are primarily an exercise of the President's authority as Commander in Chief during an armed conflict that Congress expressly has authorized the President to pursue. The NSA activities, moreover, have been undertaken specifically to prevent a renewed attack at the hands of an enemy that has already inflicted the single deadliest foreign attack in the Nation's history. The core of the Commander in Chief power is the authority to direct the Armed Forces in conducting a military campaign. Thus, the Supreme Court has made clear that the "President alone" is "constitutionally invested with the entire charge of hostile operations." *Hamilton v. Dillin*, 88 U.S. (21 Wall.) 73, 87 (1874); *The Federalist* No. 74, at 500 (Alexander Hamilton). "As commander-in-chief, [the President] is authorized to direct the movements of the naval and military forces placed by law at his command, and to employ them in the manner he may deem most effectual to harass and conquer and subdue the enemy." *Fleming v. Page*, 50 U.S. (9 How.) 603, 615 (1850). As Chief Justice Chase explained in 1866, although Congress has authority to legislate to support the prosecution of a war, Congress may not "interfere[] with the command of the forces and the conduct of campaigns. That power and duty belong to the President as commander-in-chief." *Ex parte Milligan*, 71 U.S. (4 Wall.) 2, 139 (1866) (Chase, C.J., concurring in judgment) (emphasis added).

The Executive Branch uniformly has construed the Commander in Chief and foreign affairs powers to grant the President authority that is beyond the ability of Congress to regulate. In 1860, Attorney General Black concluded that an act of Congress, if intended to constrain the President's discretion in assigning duties to an officer in the army, would be unconstitutional:

As commander-in-chief of the army it is your right to decide according to your

¹⁴ In the past, other courts have declined to express a view on that issue one way or the other. *See, e.g., Butenko*, 494 F.2d at 601 ("We do not intimate, at this time, any view whatsoever as the proper resolution of the possible clash of the constitutional powers of the President and Congress.").

own judgment what officer shall perform any particular duty, and as the supreme executive magistrate you have the power of appointment. Congress could not, if it would, take away from the President, or in anywise diminish the authority conferred upon him by the Constitution.

Memorial of Captain Meigs, 9 Op. Att'y Gen. 462, 468 (1860). Attorney General Black went on to explain that, in his view, the statute involved there could probably be read as simply providing "a recommendation" that the President could decline to follow at his discretion. *Id.* at 469-70.¹⁵

Supreme Court precedent does not support claims of congressional authority over core military decisions during armed conflicts. In particular, the two decisions of the Supreme Court that address a conflict between asserted wartime powers of the Commander in Chief and congressional legislation and that resolve the conflict in favor of Congress—*Little v. Barreme*, 6 U.S. (2 Cranch) 170 (1804), and *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579 (1952)—are both distinguishable from the situation presented by the NSA activities in the conflict with al Qaeda. Neither supports the constitutionality of the restrictions in FISA as applied here.

Barreme involved a suit brought to recover a ship seized by an officer of the U.S. Navy on the high seas during the so-called "Quasi War" with France in 1799. The seizure had been based upon the officer's orders implementing an act of Congress suspending commerce between the United States and France and authorizing the seizure of American ships bound to a French port. The ship in question was suspected of sailing from a French port. The Supreme Court held that the orders given by the President could not authorize a seizure beyond the terms of the

¹⁵ Executive practice recognizes, consistent with the Constitution, some congressional control over the Executive's decisions concerning the Armed Forces. See, e.g., U.S. Const. art. I, § 8, cl. 12 (granting Congress power "to raise and support Armies"). But such examples have not involved congressional attempts to regulate the actual conduct of a military campaign, and there is no comparable textual support for such interference. For example, just before World War II, Attorney General Robert Jackson concluded that the Neutrality Act prohibited President Roosevelt from selling certain armed naval vessels and sending them to Great Britain. See *Acquisition of Naval and Air Bases in Exchange for Over-Age Destroyers*, 39 Op. Att'y Gen. 484, 496 (1940). Jackson's apparent conclusion that Congress could control the President's ability to transfer war material does not imply acceptance of direct congressional regulation of the Commander in Chief's control of the means and methods of engaging the enemy in conflict. Similarly, in *Youngstown Sheet & Tube Co. v. Sawyer*, the Truman Administration readily conceded that, if Congress had prohibited the seizure of steel mills by statute, Congress's action would have been controlling. See Brief for Petitioner at 150, *Youngstown*, 343 U.S. 579 (1952) (Nos. 744 and 745). This concession implies nothing concerning congressional control over the methods of engaging the enemy.

Likewise, the fact that the Executive Branch has, at times, sought congressional ratification after taking unilateral action in a wartime emergency does not reflect a concession that the Executive lacks authority in this area. A decision to seek congressional support can be prompted by many motivations, including a desire for political support. In modern times, several administrations have sought congressional authorization for the use of military force while preserving the ability to assert the unconstitutionality of the War Powers Resolution. See, e.g., *Statement on Signing the Resolution Authorizing the Use of Military Force Against Iraq*, 1 Pub. Papers of George Bush 40 (1991) ("[M]y request for congressional support did not . . . constitute any change in the long-standing positions of the executive branch on either the President's constitutional authority to use the Armed Forces to defend vital U.S. interests or the constitutionality of the War Powers Resolution."). Moreover, many actions for which congressional support has been sought—such as President Lincoln's action in raising an Army in 1861—quite likely fall primarily under Congress's core Article I powers.

statute and therefore that the seizure of the ship not in fact bound to a French port was unlawful. See 6 U.S. at 177-78. Although some commentators have broadly characterized *Barreme* as standing for the proposition that Congress may restrict by statute the means by which the President can direct the Nation's Armed Forces to carry on a war, the Court's holding was limited in at least two significant ways. First, the operative section of the statute in question applied only to *American* merchant ships. See *id.* at 170 (quoting Act of February 9, 1799). Thus, the Court simply had no occasion to rule on whether, even in the limited and peculiar circumstances of the Quasi War, Congress could have placed some restriction on the orders the Commander in Chief could issue concerning direct engagements with enemy forces. Second, it is significant that the statute in *Barreme* was cast expressly, not as a limitation on the conduct of warfare by the President, but rather as regulation of a subject within the core of Congress's enumerated powers under Article I—the regulation of foreign commerce. See U.S. Const., art. I, § 8, cl. 3. The basis of Congress's authority to act was therefore clearer in *Barreme* than it is here.

Youngstown involved an effort by the President—in the face of a threatened work stoppage—to seize and to run steel mills. Congress had expressly considered the possibility of giving the President power to effect such a seizure during national emergencies. It rejected that option, however, instead providing different mechanisms for resolving labor disputes and mechanisms for seizing industries to ensure production vital to national defense.

For the Court, the connection between the seizure and the core Commander in Chief function of commanding the Armed Forces was too attenuated. The Court pointed out that the case did not involve authority over “day-to-day fighting in a theater of war.” *Id.* at 587. Instead, it involved a dramatic extension of the President's authority over military operations to exercise control over an industry that was vital for producing equipment needed overseas. Justice Jackson's concurring opinion also reveals a concern for what might be termed foreign-to-domestic presidential bootstrapping. The United States became involved in the Korean conflict through President Truman's unilateral decision to commit troops to the defense of South Korea. The President then claimed authority, based upon this foreign conflict, to extend presidential control into vast sectors of the domestic economy. Justice Jackson expressed “alarm[]” at a theory under which “a President whose conduct of foreign affairs is so largely uncontrolled, and often even is unknown, can vastly enlarge his mastery over the internal affairs of the country by his own commitment of the Nation's armed forces to some foreign venture.” *Id.* at 642.

Moreover, President Truman's action extended the President's authority into a field that the Constitution predominantly assigns to Congress. See *id.* at 588 (discussing Congress's commerce power and noting that “[t]he Constitution does not subject this lawmaking power of Congress to presidential or military supervision or control”); see also *id.* at 643 (Jackson, J., concurring) (explaining that Congress is given express authority to “raise and support Armies” and “to provide and maintain a Navy”) (quoting U.S. Const. art. I, § 8, cls. 12, 13). Thus, *Youngstown* involved an assertion of executive power that not only stretched far beyond the

President's core Commander in Chief functions, but that did so by intruding into areas where Congress had been given an express, and apparently dominant, role by the Constitution.¹⁶

The present situation differs dramatically. The exercise of executive authority involved in the NSA activities is not several steps removed from the actual conduct of a military campaign. As explained above, it is an essential part of the military campaign. Unlike the activities at issue in *Youngstown*, the NSA activities are directed at the enemy, and not at domestic activity that might incidentally aid the war effort. And assertion of executive authority here does not involve extending presidential power into areas reserved for Congress. Moreover, the theme that appeared most strongly in Justice Jackson's concurrence in *Youngstown*—the fear of presidential bootstrapping—does not apply in this context. Whereas President Truman had used his inherent constitutional authority to commit U.S. troops, here Congress expressly provided the President sweeping authority to use "all necessary and appropriate force" to protect the Nation from further attack. AUMF § 2(a). There is thus no bootstrapping concern.

Finally, *Youngstown* cannot be read to suggest that the President's authority for engaging the enemy is less extensive inside the United States than abroad. To the contrary, the extent of the President's Commander in Chief authority necessarily depends on where the enemy is found and where the battle is waged. In World War II, for example, the Supreme Court recognized that the President's authority as Commander in Chief, as supplemented by Congress, included the power to capture and try agents of the enemy in the United States, even if they never had "entered the theatre or zone of active military operations." *Quirin*, 317 U.S. at 38.¹⁷ In the present conflict, unlike in the Korean War, the battlefield was brought to the United States in the most literal way, and the United States continues to face a threat of further attacks on its soil. In short, therefore, *Youngstown* does not support the view that Congress may constitutionally prohibit the President from authorizing the NSA activities.

The second serious constitutional question is whether the particular restrictions imposed by FISA would impermissibly hamper the President's exercise of his constitutionally assigned duties as Commander in Chief. The President has determined that the speed and agility required to carry out the NSA activities successfully could not have been achieved under FISA.¹⁸ Because the President also has determined that the NSA activities are necessary to the defense of

¹⁶ *Youngstown* does demonstrate that the mere fact that Executive action might be placed in Justice Jackson's category III does not obviate the need for further analysis. Justice Jackson's framework therefore recognizes that Congress might impermissibly interfere with the President's authority as Commander in Chief or to conduct the Nation's foreign affairs.

¹⁷ It had been recognized long before *Youngstown* that, in a large-scale conflict, the area of operations could readily extend to the continental United States, even when there are no major engagements of armed forces here. Thus, in the context of the trial of a German officer for spying in World War I, it was recognized that "[w]ith the progress made in obtaining ways and means for devastation and destruction, the territory of the United States was certainly within the field of active operations" during the war, particularly in the port of New York, and that a spy in the United States might easily have aided the "hostile operation" of U-boats off the coast. *United States ex rel. Wessels v. McDonald*, 265 F. 754, 764 (E.D.N.Y. 1920).

¹⁸ In order to avoid further compromising vital national security activities, a full explanation of the basis for the President's determination cannot be given in an unclassified document.

the United States from a subsequent terrorist attack in the armed conflict with al Qaeda, FISA would impermissibly interfere with the President's most solemn constitutional obligation—to defend the United States against foreign attack.

Indeed, if an interpretation of FISA that allows the President to conduct the NSA activities were not “fairly possible,” FISA would be unconstitutional as applied in the context of this congressionally authorized armed conflict. In that event, FISA would purport to *prohibit* the President from undertaking actions necessary to fulfill his constitutional obligation to protect the Nation from foreign attack in the context of a congressionally authorized armed conflict with an enemy that has already staged the most deadly foreign attack in our Nation's history. A statute may not “*impede* the President's ability to perform his constitutional duty,” *Morrison v. Olson*, 487 U.S. 654, 691 (1988) (emphasis added); *see also id.* at 696-97, particularly not the President's most solemn constitutional obligation—the defense of the Nation. *See also In re Sealed Case*, 310 F.3d at 742 (explaining that “FISA could not encroach on the President's constitutional power”).

Application of the avoidance canon would be especially appropriate here for several reasons beyond the acute constitutional crises that would otherwise result. First, as noted, Congress did not intend FISA to be the final word on electronic surveillance conducted during armed conflicts. Instead, Congress expected that it would revisit the subject in subsequent legislation. Whatever intent can be gleaned from FISA's text and legislative history to set forth a comprehensive scheme for regulating electronic surveillance during peacetime, that same intent simply does not extend to armed conflicts and declared wars.¹⁹ Second, FISA was enacted during the Cold War, not during active hostilities with an adversary whose mode of operation is to blend in with the civilian population until it is ready to strike. These changed circumstances have seriously altered the constitutional calculus, one that FISA's enactors had already recognized might suggest that the statute was unconstitutional. Third, certain technological changes have rendered FISA still more problematic. As discussed above, when FISA was enacted in 1978, Congress expressly declined to regulate through FISA certain signals intelligence activities conducted by the NSA. *See supra*, at pp. 18-19 & n.6.²⁰ These same factors weigh heavily in favor of concluding that FISA would be unconstitutional as applied to the current conflict if the canon of constitutional avoidance could not be used to head off a collision between the Branches.

¹⁹ FISA exempts the President from its procedures for fifteen days following a congressional declaration of war. *See* 50 U.S.C. § 1811. If an adversary succeeded in a decapitation strike, preventing Congress from declaring war or passing subsequent authorizing legislation, it seems clear that FISA could not constitutionally continue to apply in such circumstances.

²⁰ Since FISA's enactment in 1978, the means of transmitting communications has undergone extensive transformation. In particular, many communications that would have been carried by wire are now transmitted through the air, and many communications that would have been carried by radio signals (including by satellite transmissions) are now transmitted by fiber optic cables. It is such technological advancements that have broadened FISA's reach, not any particularized congressional judgment that the NSA's traditional activities in intercepting such international communications should be subject to FISA's procedures. A full explanation of these technological changes would require a discussion of classified information.

* * *

As explained above, FISA is best interpreted to allow a statute such as the AUMF to authorize electronic surveillance outside FISA's enumerated procedures. The strongest counterarguments to this conclusion are that various provisions in FISA and title 18, including section 111 of FISA and section 2511(2)(f) of title 18, together require that subsequent legislation must reference or amend FISA in order to authorize electronic surveillance outside FISA's procedures and that interpreting the AUMF as a statute authorizing electronic surveillance outside FISA procedures amounts to a disfavored repeal by implication. At the very least, however, interpreting FISA to allow a subsequent statute such as the AUMF to authorize electronic surveillance without following FISA's express procedures is "fairly possible," and that is all that is required for purposes of invoking constitutional avoidance. In the competition of competing canons, particularly in the context of an ongoing armed conflict, the constitutional avoidance canon carries much greater interpretative force.²¹

IV. THE NSA ACTIVITIES ARE CONSISTENT WITH THE FOURTH AMENDMENT

The Fourth Amendment prohibits "unreasonable searches and seizures" and directs that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and

²¹ If the text of FISA were clear that nothing other than an amendment to FISA could authorize additional electronic surveillance, the AUMF would impliedly repeal as much of FISA as would prevent the President from using "all necessary and appropriate force" in order to prevent al Qaeda and its allies from launching another terrorist attack against the United States. To be sure, repeals by implication are disfavored and are generally not found whenever two statutes are "capable of co-existence." *Ruckelshaus v. Monsanto Co.*, 467 U.S. 986, 1018 (1984). Under this standard, an implied repeal may be found where one statute would "unduly interfere with" the operation of another. *Radzanower v. Touche Ross & Co.*, 426 U.S. 148, 156 (1976). The President's determination that electronic surveillance of al Qaeda outside the confines of FISA was "necessary and appropriate" would create a clear conflict between the AUMF and FISA. FISA's restrictions on the use of electronic surveillance would preclude the President from doing what the AUMF specifically authorized him to do: use all "necessary and appropriate force" to prevent al Qaeda from carrying out future attacks against the United States. The ordinary restrictions in FISA cannot continue to apply if the AUMF is to have its full effect; those constraints would "unduly interfere" with the operation of the AUMF.

Contrary to the recent suggestion made by several law professors and former government officials, the ordinary presumption against implied repeals is overcome here. *Cf.* Letter to the Hon. Bill Frist, Majority Leader, U.S. Senate, from Professor Curtis A. Bradley et al. at 4 (Jan. 9, 2006). First, like other canons of statutory construction, the canon against implied repeals is simply a presumption that may be rebutted by other factors, including conflicting canons. *Connecticut National Bank v. Germain*, 503 U.S. 249, 253 (1992); *see also Chickasaw Nation v. United States*, 534 U.S. 84, 94 (2001); *Circuit City Stores, Inc. v. Adams*, 532 U.S. 105, 115 (2001). Indeed, the Supreme Court has declined to apply the ordinary presumption against implied repeals where other canons apply and suggest the opposite result. *See Montana v. Blackfeet Tribe of Indians*, 471 U.S. 759, 765-66 (1985). Moreover, *Blackfeet* suggests that where the presumption against implied repeals would conflict with other, more compelling interpretive imperatives, it simply does not apply at all. *See* 471 U.S. at 766. Here, in light of the constitutional avoidance canon, which imposes the overriding imperative to use the tools of statutory interpretation to avoid constitutional conflicts, the implied repeal canon either would not apply at all or would apply with significantly reduced force. Second, the AUMF was enacted during an acute national emergency, where the type of deliberation and detail normally required for application of the canon against implied repeals was neither practical nor warranted. As discussed above, in these circumstances, Congress cannot be expected to work through every potential implication of the U.S. Code and to define with particularity each of the traditional incidents of the use of force available to the President.

particularly describing the place to be searched, and the persons or things to be seized.” U.S. Const. amend. IV. The touchstone for review of government action under the Fourth Amendment is whether the search is “reasonable.” See, e.g., *Vernonia Sch. Dist. v. Acton*, 515 U.S. 646, 653 (1995).

As noted above, see Part I, all of the federal courts of appeals to have addressed the issue have affirmed the President’s inherent constitutional authority to collect foreign intelligence without a warrant. See *In re Sealed Case*, 310 F.3d at 742. Properly understood, foreign intelligence collection in general, and the NSA activities in particular, fit within the “special needs” exception to the warrant requirement of the Fourth Amendment. Accordingly, the mere fact that no warrant is secured prior to the surveillance at issue in the NSA activities does not suffice to render the activities unreasonable. Instead, reasonableness in this context must be assessed under a general balancing approach, “by assessing, on the one hand, the degree to which it intrudes upon an individual’s privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.” *United States v. Knights*, 534 U.S. 112, 118-19 (2001) (quoting *Wyoming v. Houghton*, 526 U.S. 295, 300 (1999)). The NSA activities are reasonable because the Government’s interest, defending the Nation from another foreign attack in time of armed conflict, outweighs the individual privacy interests at stake, and because they seek to intercept only international communications where one party is linked to al Qaeda or an affiliated terrorist organization.

A. THE WARRANT REQUIREMENT OF THE FOURTH AMENDMENT DOES NOT APPLY TO THE NSA ACTIVITIES

In “the criminal context,” the Fourth Amendment reasonableness requirement “usually requires a showing of probable cause” and a warrant. *Board of Educ. v. Earls*, 536 U.S. 822, 828 (2002). The requirement of a warrant supported by probable cause, however, is not universal. Rather, the Fourth Amendment’s “central requirement is one of reasonableness,” and the rules the Court has developed to implement that requirement “[s]ometimes . . . require warrants.” *Illinois v. McArthur*, 531 U.S. 326, 330 (2001); see also, e.g., *Earls*, 536 U.S. at 828 (noting that the probable cause standard “is peculiarly related to criminal investigations and may be unsuited to determining the reasonableness of administrative searches where the Government seeks to prevent the development of hazardous conditions”) (internal quotation marks omitted).

In particular, the Supreme Court repeatedly has made clear that in situations involving “special needs” that go beyond a routine interest in law enforcement, the warrant requirement is inapplicable. See *Vernonia*, 515 U.S. at 653 (there are circumstances “when special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable”) (quoting *Griffin v. Wisconsin*, 483 U.S. 868, 873 (1987)); see also *McArthur*, 531 U.S. at 330 (“When faced with special law enforcement needs, diminished expectations of privacy, minimal intrusions, or the like, the Court has found that certain general, or individual, circumstances may render a warrantless search or seizure reasonable.”). It is difficult to encapsulate in a nutshell all of the different circumstances the Court has found to qualify as “special needs” justifying warrantless searches. But one application in which the Court has found the warrant requirement inapplicable is in circumstances in which the Government faces

an increased need to be able to react swiftly and flexibly, or when there are at stake interests in public safety beyond the interests in ordinary law enforcement. One important factor in establishing "special needs" is whether the Government is responding to an emergency that goes beyond the need for general crime control. See *In re Sealed Case*, 310 F.3d at 745-46.

Thus, the Court has permitted warrantless searches of property of students in public schools, see *New Jersey v. T.L.O.*, 469 U.S. 325, 340 (1985) (noting that warrant requirement would "unduly interfere with the maintenance of the swift and informal disciplinary procedures needed in the schools"), to screen athletes and students involved in extracurricular activities at public schools for drug use, see *Vernonia*, 515 U.S. at 654-55; *Earls*, 536 U.S. at 829-38, to conduct drug testing of railroad personnel involved in train accidents, see *Skinner v. Railway Labor Executives' Ass'n*, 489 U.S. 602, 634 (1989), and to search probationers' homes, see *Griffin*, 483 U.S. 868. Many special needs doctrine and related cases have upheld *suspicionless* searches or seizures. See, e.g., *Illinois v. Lidster*, 540 U.S. 419, 427 (2004) (implicitly relying on special needs doctrine to uphold use of automobile checkpoint to obtain information about recent hit-and-run accident); *Earls*, 536 U.S. at 829-38 (suspicionless drug testing of public school students involved in extracurricular activities); *Michigan Dep't of State Police v. Sitz*, 496 U.S. 444, 449-55 (1990) (road block to check all motorists for signs of drunken driving); *United States v. Martinez-Fuerte*, 428 U.S. 543 (1976) (road block near the border to check vehicles for illegal immigrants); cf. *In re Sealed Case*, 310 F.3d at 745-46 (noting that suspicionless searches and seizures in one sense are a greater encroachment on privacy than electronic surveillance under FISA because they are not based on any particular suspicion, but "[o]n the other hand, wiretapping is a good deal more intrusive than an automobile stop accompanied by questioning"). To fall within the "special needs" exception to the warrant requirement, the purpose of the search must be distinguishable from ordinary general crime control. See, e.g., *Ferguson v. Charleston*, 532 U.S. 67 (2001); *City of Indianapolis v. Edmond*, 531 U.S. 32, 41 (2000).

Foreign intelligence collection, especially in the midst of an armed conflict in which the adversary has already launched catastrophic attacks within the United States, fits squarely within the area of "special needs, beyond the normal need for law enforcement" where the Fourth Amendment's touchstone of reasonableness can be satisfied without resort to a warrant. *Vernonia*, 515 U.S. at 653. The Executive Branch has long maintained that collecting foreign intelligence is far removed from the ordinary criminal law enforcement action to which the warrant requirement is particularly suited. See, e.g., *Amending the Foreign Intelligence Surveillance Act: Hearings Before the House Permanent Select Comm. on Intelligence*, 103d Cong. 2d Sess. 62, 63 (1994) (statement of Deputy Attorney General Jamie S. Gorelick) ("[I]t is important to understand that the rules and methodology for criminal searches are inconsistent with the collection of foreign intelligence and would unduly frustrate the President in carrying out his foreign intelligence responsibilities. . . . [W]e believe that the warrant clause of the Fourth Amendment is inapplicable to such [foreign intelligence] searches."); see also *In re Sealed Case*, 310 F.3d 745. The object of foreign intelligence collection is securing information necessary to protect the national security from the hostile designs of foreign powers like al Qaeda and affiliated terrorist organizations, including the possibility of another foreign attack on the United States. In foreign intelligence investigations, moreover, the targets of surveillance

often are agents of foreign powers, including international terrorist groups, who may be specially trained in concealing their activities and whose activities may be particularly difficult to detect. The Executive requires a greater degree of flexibility in this field to respond with speed and absolute secrecy to the ever-changing array of foreign threats faced by the Nation.²²

In particular, the NSA activities are undertaken to prevent further devastating attacks on our Nation, and they serve the highest government purpose through means other than traditional law enforcement.²³ The NSA activities are designed to enable the Government to act quickly and flexibly (and with secrecy) to find agents of al Qaeda and its affiliates—an international terrorist group which has already demonstrated a capability to infiltrate American communities without being detected—in time to disrupt future terrorist attacks against the United States. As explained by the Foreign Intelligence Surveillance Court of Review, the nature of the “emergency” posed by al Qaeda “takes the matter out of the realm of ordinary crime control.” *In re Sealed Case*, 310 F.3d at 746. Thus, under the “special needs” doctrine, no warrant is required by the Fourth Amendment for the NSA activities.

B. THE NSA ACTIVITIES ARE REASONABLE

As the Supreme Court has emphasized repeatedly, “[t]he touchstone of the Fourth Amendment is reasonableness, and the reasonableness of a search is determined by assessing, on the one hand, the degree to which it intrudes upon an individual’s privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.” *Knights*, 534 U.S. at 118-19 (quotation marks omitted); see also *Earls*, 536 U.S. at 829. The Supreme Court has found a search reasonable when, under the totality of the circumstances, the importance of the governmental interests outweighs the nature and quality of the intrusion on the individual’s Fourth Amendment interests. See *Knights*, 534 U.S. at 118-22. Under the standard

²² Even in the domestic context, the Supreme Court has recognized that there may be significant distinctions between wiretapping for ordinary law enforcement purposes and domestic national security surveillance. See *United States v. United States District Court*, 407 U.S. 297, 322 (1972) (“*Keith*”) (explaining that “the focus of domestic [security] surveillance may be less precise than that directed against more conventional types of crime” because often “the emphasis of domestic intelligence gathering is on the prevention of unlawful activity or the enhancement of the Government’s preparedness for some possible future crisis or emergency”); see also *United States v. Duggan*, 743 F.2d 59, 72 (2d Cir. 1984) (reading *Keith* to recognize that “the governmental interests presented in national security investigations differ substantially from those presented in traditional criminal investigations”). Although the Court in *Keith* held that the Fourth Amendment’s warrant requirement does apply to investigations of purely domestic threats to national security—such as domestic terrorism, it suggested that Congress consider establishing a lower standard for such warrants than that set forth in Title III. See *id.* at 322-23 (advising that “different standards” from those applied to traditional law enforcement “may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of the Government for intelligence information and the protected rights of our citizens”). *Keith*’s emphasis on the need for flexibility applies with even greater force to surveillance directed at foreign threats to national security. See S. Rep. No. 95-701, at 16 (“Far more than in domestic security matters, foreign counterintelligence investigations are ‘long range’ and involve ‘the interrelation of various sources and types of information.’”) (quoting *Keith*, 407 U.S. at 322). And flexibility is particularly essential here, where the purpose of the NSA activities is to prevent another armed attack against the United States.

²³ This is not to say that traditional law enforcement has no role in protecting the Nation from attack. The NSA activities, however, are not directed at bringing criminals to justice but at detecting and preventing plots by a declared enemy of the United States to attack it again.

balancing of interests analysis used for gauging reasonableness, the NSA activities are consistent with the Fourth Amendment.

With respect to the individual privacy interests at stake, there can be no doubt that, as a general matter, interception of telephone communications implicates a significant privacy interest of the individual whose conversation is intercepted. The Supreme Court has made clear at least since *Katz v. United States*, 389 U.S. 347 (1967), that individuals have a substantial and constitutionally protected reasonable expectation of privacy that their telephone conversations will not be subject to governmental eavesdropping. Although the individual privacy interests at stake may be substantial, it is well recognized that a variety of governmental interests—including routine law enforcement and foreign-intelligence gathering—can overcome those interests.

On the other side of the scale here, the Government's interest in engaging in the NSA activities is the most compelling interest possible—securing the Nation from foreign attack in the midst of an armed conflict. One attack already has taken thousands of lives and placed the Nation in state of armed conflict. Defending the Nation from attack is perhaps the most important function of the federal Government—and one of the few express obligations of the federal Government enshrined in the Constitution. *See* U.S. Const. art. IV, § 4 (“The United States shall guarantee to every State in this Union a Republican Form of Government, and shall protect each of them against Invasion . . .”) (emphasis added); *The Prize Cases*, 67 U.S. (2 Black) 635, 668 (1863) (“If war be made by invasion of a foreign nation, the President is not only authorized but bound to resist force by force.”). As the Supreme Court has declared, “[i]t is ‘obvious and unarguable’ that no governmental interest is more compelling than the security of the Nation.” *Haig v. Agee*, 453 U.S. 280, 307 (1981).

The Government's overwhelming interest in detecting and thwarting further al Qaeda attacks is easily sufficient to make reasonable the intrusion into privacy involved in intercepting one-end foreign communications where there is “a reasonable basis to conclude that one party to the communication is a member of al Qaeda, affiliated with al Qaeda, or a member of an organization affiliated with al Qaeda.” Press Briefing by Attorney General Alberto Gonzales and General Michael Hayden, Principal Deputy Director for National Intelligence, available at <http://www.whitehouse.gov/news/releases/2005/12/20051219-1.html> (Dec. 19, 2005) (statement of Attorney General Gonzales); *cf. Edmond*, 531 U.S. at 44 (noting that “the Fourth Amendment would almost certainly permit an appropriately tailored roadblock set up to thwart an imminent terrorist attack” because “[t]he exigencies created by th[at] scenario[] are far removed” from ordinary law enforcement). The United States has already suffered one attack that killed thousands, disrupted the Nation's financial center for days, and successfully struck at the command and control center for the Nation's military. And the President has stated that the NSA activities are “critical” to our national security. Press Conference of President Bush (Dec. 19, 2005). To this day, finding al Qaeda sleeper agents in the United States remains one of the preeminent concerns of the war on terrorism. As the President has explained, “[t]he terrorists want to strike America again, and they hope to inflict even more damage than they did on September 11th.” *Id.*

Of course, because the magnitude of the Government's interest here depends in part upon the threat posed by al Qaeda, it might be possible for the weight that interest carries in the balance to change over time. It is thus significant for the reasonableness of the NSA activities that the President has established a system under which he authorizes the surveillance only for a limited period, typically for 45 days. This process of reauthorization ensures a periodic review to evaluate whether the threat from al Qaeda remains sufficiently strong that the Government's interest in protecting the Nation and its citizens from foreign attack continues to outweigh the individual privacy interests at stake.

Finally, as part of the balancing of interests to evaluate Fourth Amendment reasonableness, it is significant that the NSA activities are limited to intercepting international communications where there is a reasonable basis to conclude that one party to the communication is a member or agent of al Qaeda or an affiliated terrorist organization. This factor is relevant because the Supreme Court has indicated that in evaluating reasonableness, one should consider the "efficacy of [the] means for addressing the problem." *Vernonia*, 515 U.S. at 663; *see also Earls*, 536 U.S. at 834 ("Finally, this Court must consider the nature and immediacy of the government's concerns and the efficacy of the Policy in meeting them."). That consideration does not mean that reasonableness requires the "least intrusive" or most "narrowly tailored" means for obtaining information. To the contrary, the Supreme Court has repeatedly rejected such suggestions. *See, e.g., Earls*, 536 U.S. at 837 ("[T]his Court has repeatedly stated that reasonableness under the Fourth Amendment does not require employing the least intrusive means, because the logic of such elaborate less-restrictive-alternative arguments could raise insuperable barriers to the exercise of virtually all search-and-seizure powers.") (internal quotation marks omitted); *Vernonia*, 515 U.S. at 663 ("We have repeatedly refused to declare that only the 'least intrusive' search practicable can be reasonable under the Fourth Amendment."). Nevertheless, the Court has indicated that some consideration of the efficacy of the search being implemented—that is, some measure of fit between the search and the desired objective—is relevant to the reasonableness analysis. The NSA activities are targeted to intercept international communications of persons reasonably believed to be members or agents of al Qaeda or an affiliated terrorist organization, a limitation which further strongly supports the reasonableness of the searches.

In sum, the NSA activities are consistent with the Fourth Amendment because the warrant requirement does not apply in these circumstances, which involve both "special needs" beyond the need for ordinary law enforcement and the inherent authority of the President to conduct warrantless electronic surveillance to obtain foreign intelligence to protect our Nation from foreign armed attack. The touchstone of the Fourth Amendment is reasonableness, and the NSA activities are certainly reasonable, particularly taking into account the nature of the threat the Nation faces.

CONCLUSION

For the foregoing reasons, the President—in light of the broad authority to use military force in response to the attacks of September 11th and to prevent further catastrophic attack expressly conferred on the President by the Constitution and confirmed and supplemented by

Congress in the AUMF—has legal authority to authorize the NSA to conduct the signals intelligence activities he has described. Those activities are authorized by the Constitution and by statute, and they violate neither FISA nor the Fourth Amendment.

EXHIBIT B

RECEIVED
CLERK'S OFFICE

2006 MAY 24 P 3:08

JUDICIAL PANEL ON
MULTIDISTRICT
LITIGATION

**BEFORE THE JUDICIAL PANEL
ON MULTIDISTRICT LITIGATION**

IN RE NATIONAL SECURITY AGENCY)
LITIGATION)
_____)

MDL Docket No. _____

**DEFENDANTS VERIZON COMMUNICATIONS INC., VERIZON GLOBAL
NETWORKS INC., AND VERIZON NORTHWEST INC.'S MOTION FOR TRANSFER
AND COORDINATION PURSUANT TO 28 U.S.C. § 1407**

Defendants Verizon Communications Inc., Verizon Global Networks Inc., and Verizon Northwest Inc. (collectively "Verizon") hereby respectfully move the Judicial Panel on Multidistrict Litigation for an order: (a) transferring 20 virtually identical purported class actions (pending before 14 different federal district courts) to a single district court; and (b) coordinating those actions for pretrial proceedings pursuant to 28 U.S.C. § 1407. A list of the 20 pending actions, 19 of which have been filed in the last two weeks, is attached hereto as Verizon's Schedule of National Security Agency Actions for Transfer and Coordination.

In support of the transfer and coordination of these actions, the movants aver the following, as more fully set forth in the accompanying supporting memorandum:

1. The actions for which transfer and coordination is proposed allege participation by Verizon in a Government program to intercept and analyze domestic telephone and Internet

communications as reported in a U.S.A. Today article published on May 11, 2006. All save one of these actions have been filed within two weeks since that article was published. Plaintiffs in each case claim that Verizon and other telecommunication company defendants assisted the Government in its intelligence efforts by providing the Government, at the request of the National Security Agency, with information concerning their customers' telephone and internet communications and detailed records of their customers' telephone calls. All but one of the proposed classes seek relief under the Electronic Communications Privacy Act, 18 U.S.C. § 2701 *et seq.* Most of the cases propose nationwide classes comprising all of Verizon's or other providers' subscribing customers; five cases propose regional classes or classes without precise definition.

2. As required by 28 U.S.C. § 1407(a), the cases proposed for transfer and coordination "involv[e] one or more common questions of fact" inasmuch as they are premised on identical factual allegations, contending that Verizon disclosed records pertaining to plaintiffs' use of Verizon's telecommunications services to the National Security Agency, that Verizon disclosed the records without the knowledge or consent of its customers, and that it did so without authorization or a warrant.¹

3. In multiple respects, the proposed transfer and coordination "will be for the convenience of parties and witnesses and will promote the just and efficient conduct" of the actions. 28 U.S.C. § 1407(a).

¹ By asserting that the Section 1407 standard has been satisfied to warrant multidistrict transfer, movants do not address whether or concede that the requirements for class certification, including, but not limited to, the commonality and/or the predominance requirements, have been met. The Section 1407 inquiry is distinct from analysis of the class certification criteria, and is applied by courts with different purposes in mind. As the Manual for Complex Litigation makes clear, one of the main objectives of a multidistrict transfer is pretrial administrative efficiency. See MANUAL FOR COMPLEX LITIGATION § 10.1 (4th ed. 2004). Whether the case should be certified as a class action and proceed to trial on that basis is a different inquiry altogether. For purposes of this motion, movants demonstrate only that the actions should be coordinated for Section 1407 purposes.

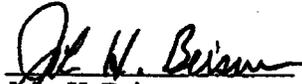
4. For example, coordination of the actions before a single court will eliminate duplicative discovery activity (particularly multiple depositions of the same witnesses) and concomitantly minimize the potential disclosure of classified information, prevent duplicative and conflicting pretrial rulings, conserve judicial resources, reduce the costs of litigation, and allow the cases to proceed more efficiently to trial. Coordination will also protect unique national security interests that will color discovery in this action.

5. Defendants respectfully suggest that the U.S. District Court for the District of Columbia would be an appropriate transferee forum. Three related cases – *Driscoll v. Verizon Communications, Inc.*, No. 06-cv-916, *Ludman v. AT&T Inc.*, No. 06-cv-917, and *Phillips v. BellSouth Corp.*, 06-cv-918 – are pending before that Court, and the forum would be a convenient one for counsel and for the defendants. Moreover, the U.S. District Court for the District of Columbia has fewer cases pending before it than any other federal courts in which a National Security Agency case is currently pending save one and has substantial expertise in dealing with the national-security and state-secrets issues inherent in these cases.

6. This Motion is based on the Brief in Support of this Motion to Transfer and Coordinate filed by Verizon, the pleadings and papers on file herein, and such other matters as may be presented to the Panel at the time of hearing.

Dated: May 24, 2006

Respectfully submitted,



John H. Beisner
Brian D. Boyle
Thomas E. Donilon
Matthew M. Shors
O'MELVENY AND MYERS LLP
1625 Eye Street, NW
Washington, DC 20006
(202) 383-5300 (phone)
(202) 383-5414 (fax)



John A. Rogovin
Randolph D. Moss
Samir Jain
Brian Boynton
WILMER CUTLER PICKERING HALE AND
DORR LLP
1875 Pennsylvania Avenue, N.W.
Washington, DC 20006
(202) 663-6000 (phone)
(202) 663-6363 (fax)

*Attorneys for Verizon Communications Inc., Verizon Global Networks Inc., and Verizon
Northwest Inc.*

RECEIVED
CLERK'S OFFICE

2006 MAY 24 P 3: 08

JUDICIAL PANEL ON
MULTIDISTRICT
LITIGATION

**BEFORE THE JUDICIAL PANEL
ON MULTIDISTRICT LITIGATION**

IN RE NATIONAL SECURITY)
AGENCY LITIGATION)
_____)

MDL Docket No. _____

**MEMORANDUM IN SUPPORT OF DEFENDANTS VERIZON COMMUNICATIONS
INC., VERIZON GLOBAL NETWORKS INC., AND VERIZON NORTHWEST INC.'S
MOTION FOR TRANSFER AND COORDINATION PURSUANT TO 28 U.S.C. § 1407**

Pursuant to 28 U.S.C. § 1407 and Rule 7.1(b) of the Rules of Procedure of the Judicial Panel on Multidistrict Litigation, Verizon Communications Inc., Verizon Global Networks Inc., and Verizon Northwest Inc. – collectively “Verizon” – seek transfer and pretrial coordination of 20 class action lawsuits filed against Verizon and other defendants, the majority of which seek nationwide class certification and were filed within the past two weeks on the basis of the same factual allegations.¹ A multidistrict litigation (“MDL”) proceeding is warranted because all of the statutory criteria for transfer and coordination are present.

¹ The cases in which Verizon is a named defendant are *Bissitt v. Verizon Communications, Inc.*, No. 1:06-cv-00220-T-LDA (D.R.I.); *Conner v. AT&T*, No. 06-0225 (E.D. Cal.); *Driscoll v. Verizon Communications, Inc.*, No. 1:06-cv-00916-RBW (D.D.C.); *Fuller v. Verizon Communications, Inc.*, No. 9:06-cv-00077-DWM (D. Mont.); *Herron v. Verizon Global Networks, Inc.*, No. 2:06-cv-02491-JCZ-KWR (E.D. La.); *Hines v. Verizon Northwest, Inc.*, No. 9:06-cv-00694 (D. Or.); *Mahoney v. Verizon Communications, Inc.*, No. 1:06-cv-00224-S-LDA (D.R.I.); *Marck v. Verizon Communications, Inc.*, No. CV-06-2455 (E.D.N.Y.); *Mayer v. Verizon Communications, Inc.*, No. 1:06-cv-03650 (S.D.N.Y.). Verizon may notify the Panel of and move to transfer cases in which it is not a party if otherwise appropriate under 28 U.S.C. § 1407. *In re Cable Tie Patent Litigation*, 487 F. Supp. 1351, 1353 n.3 (J.P.M.L. 1980). Those other cases are *Dolberg v. AT&T Corp.*, No. CV 06-78-M-DWM (D. Mont.); *Harrington v.*

First, the core allegations underlying each of these purported class actions are common. All plaintiffs allege that, following the terrorist attacks on the United States on September 11, 2001, Verizon and other telecommunications companies cooperated in a Government program that involved providing the National Security Agency (“NSA”) with access to the content of their subscribers’ telephone calls and/or records concerning those calls. Indeed, all but one of the lawsuits were clearly prompted by the same article appearing in the *USA Today* on May 11, 2006.

Second, not only are the factual allegations underlying these complaints common, so too are the causes of action asserted. Each complaint alleges that the defendants violated one or more federal statutes concerning electronic surveillance and similar activities. Coordinated proceedings are warranted to benefit the parties and the federal courts alike, and to eliminate the possibility of inconsistent pretrial rulings.

Third, the proposed class definitions overlap substantially. The majority of the complaints seek certification of nationwide classes of telephone customers, while the remainder seek to certify geographically defined subsets of those putative classes. Absent centralization, multiple federal judges will be required to decide the same issues with respect to the same plaintiffs and the same defendants.

Fourth, the United States is likely to intervene in and seek dismissal of these cases – as it already has in the one and only case filed prior to the May 11, 2006 article in the *USA Today* – in order to assert its “state secret” privilege and prevent any disclosure of highly classified

AT&T, Inc., No. A06CA374-LY (W.D. Tex.); *Ludman v. AT&T Inc.*, No. 1:06-cv-00917-RBW (D.D.C.); *Mahoney v. AT&T Communications, Inc.*, No. 1:06-cv-00223-T-LDA (D.R.I.); *Schwarz v. AT&T Corp.*, No. 1:06-cv-02680 (N.D. Ill.); *Souder v. AT&T, Corp.*, No. 06CV1058-DMS AJB (S.D. Cal.); *Trevino v. AT&T Corp.*, No. 2:06-cv-00209 (S.D. Tex.); *Terkel v. AT&T Inc.*, No. 06C-2837 (N.D. Ill.); *Phillips v. BellSouth Corp.*, No. 3:06-CV-00469 (D.D.C.); *Potter v. BellSouth Corp.*, No. 3 06-0469 (M.D. Tenn.); *Hepting v. AT&T Corp.*, No. 06-0672 (N.D. Cal.). All complaints are attached hereto at Tab A.

information critical to both the plaintiffs' and defendants' cases.² There is no reason to require litigation involving important matters of national security to remain pending in various courts around the country.

For these reasons, these complaints present *the* classic case for transfer and coordination:

(i) they “involv[e] one or more common questions of fact”; (ii) transfer will further “the convenience of the parties and witnesses”; and (iii) transfer “will promote the just and efficient conduct of [the] actions by” reducing the risk of inconsistent rulings on critical pretrial matters affecting national security and the national telecommunications network, avoiding duplicative proceedings, and ensuring centralized oversight of any pretrial fact development.

Verizon respectfully submits that these cases are especially appropriate for transfer to the United States District Court for the District of Columbia. Three constituent actions are already pending there, and the District of Columbia District Court and the United States Court of Appeals for the District of Columbia Circuit both have significant experience in handling cases involving national security. Any Government witnesses and documents will likely be located in or near the District of Columbia. Similarly, classified information that may require *in camera* inspection can be maintained in highly secured locations in the District of Columbia – a factor that few other venues can offer. Finally, the case-load of the District of Columbia renders that Court more than capable of taking on this MDL proceeding.

Background

These cases concern an alleged national security program involving the collection and analysis of telephone and Internet communications.³ There is little doubt that they share

² See Notice of Motion and Motion to Dismiss or, in the Alternative, for Summary Judgment by the United States of America, *Hepting*, 3:06-CV-0672-VRW (D.D.C., filed May 13, 2006), attached hereto at Tab B.

³ See, e.g., *Driscoll* Compl. ¶ 1.

“common” factual underpinnings. Nineteen of the 20 cases Verizon seeks to transfer and coordinate have been filed since May 11, 2006, when the *USA Today* reported that the National Security Agency (“NSA”) was allegedly engaged in a classified program to amass a database including information about the calling records of millions of Americans. The article claimed that the NSA sought the help of telecommunications companies in the Government’s efforts to identify terrorists both inside and outside the United States. According to the article, Verizon, AT&T Corp. (“AT&T”), and BellSouth Corp. (“BellSouth”) all agreed to assist the Government in its efforts by providing the NSA with the call records of many of its customers.

Literally the next day, six complaints were filed against Verizon and other defendants. And in the eleven days since then, 13 additional complaints have been filed. All told, the following 20 putative class action complaints are now pending in various district courts:

- *Bissitt v. Verizon Communications, Inc.*, No. 1:06-cv-00220-T-LDA (D.R.I., filed May 15, 2006), was filed in the District of Rhode Island against Verizon Communications Inc. and BellSouth Corp. The complaint alleges that defendants disclosed plaintiffs’ telephone and internet communications records to the Government. The complaint asserts violations of the Electronic Communications Privacy Act and the First and Fourth Amendments on behalf of all subscribers of defendants’ telephonic and/or communications services since September 2001.
- *Driscoll v. Verizon Communications, Inc.*, No. 1:06-cv-00916-RBW (D.D.C., filed May 15, 2006), was filed in the District of Columbia against Verizon Communications Inc. The complaint alleges that Verizon disclosed plaintiffs’ telephone and internet communications records to the Government. The complaint asserts violations of the Electronic Communications Privacy Act on behalf of all subscribers of Verizon’s telephone and internet services since September 2001.
- *Fuller v. Verizon Communications, Inc.*, No. 9:06-cv-00077-DWM (D. Mont., filed May 12, 2006), was filed in the District of Montana against Verizon Communications Inc. and Verizon Wireless, L.L.C. The complaint alleges that the defendants disclosed plaintiff’s telephone and internet communications records to the Government. The complaint asserts violations of the Electronic Communications Privacy Act on behalf of all subscribers of defendants’ telephone and internet services since September 2001.
- *Herron v. Verizon Global Networks, Inc.*, No. 2:06-cv-02491-JCZ-KWR (E.D. La., filed May 12, 2006), was filed in the Eastern District of Louisiana against Verizon Global Networks Inc., AT&T Corp., American Telephone and Telegraph Company,

BellSouth Communication Systems, LLC, and BellSouth Telecommunications, Inc. The complaint alleges that defendants disclosed plaintiffs' telephone and internet communications records to the Government. The complaint asserts violations of the Electronic Communications Privacy Act on behalf of all persons and other entities whose phone records have allegedly been disclosed by defendants to the NSA.

- *Hines v. Verizon Northwest, Inc.*, No. 9:06-cv-00694 (D. Or., filed May 12, 2006), was filed in the District of Oregon against Verizon Northwest Inc. The complaint alleges that Verizon disclosed plaintiffs' telephone and internet communications records to the Government. The complaint asserts violations of the Electronic Communications Privacy Act on behalf of all persons within Oregon, Washington, Idaho, and California who subscribed to Verizon's electronic communication services since September 11, 2001.
- *Mahoney v. Verizon Communications, Inc.*, No. 1:06-cv-00224-S-LDA (D.R.I., filed May 15, 2006), was filed in the District of Rhode Island against Verizon Communications Inc. The complaint alleges that Verizon disclosed plaintiff's telephone and internet communications records to the Government. The complaint asserts violations of the Electronic Communications Privacy Act on behalf of all subscribers of Verizon's telephone and internet services since September 2001.
- *Marck v. Verizon Communications, Inc.*, No. CV-06-2455 (E.D.N.Y., filed May 19, 2006), was filed in the Eastern District of New York against Verizon Communications Inc. The complaint alleges that Verizon disclosed plaintiffs' telephone communications records to the Government. The complaint asserts violations of the Electronic Communications Privacy Act and the First and Fourth Amendments on behalf of all subscribers of Verizon's telephone and internet services since September 11, 2001. The complaint also asserts violations of New York's consumer protection statute on behalf of a sub-class of all New York resident subscribers of Verizon services since September 11, 2001.
- *Mayer v. Verizon Communications, Inc.*, No. 1:06-cv-03650 (S.D.N.Y., filed May 12, 2006), was filed in the Southern District of New York against Verizon Communications Inc. The complaint alleges that Verizon disclosed plaintiffs' telephone and internet communications records to the Government. The complaint asserts violations of the Electronic Communications Privacy Act and the First and Fourth Amendments on behalf of all, though possibly only New Jersey, subscribers of Verizon's telephone and internet services since September 2001.
- *Conner v. AT&T*, No. 06-0225 (E.D. Cal., removed May 23, 2006), was filed in the Superior Court of California, and later removed to the Eastern District of California, against AT&T, BellSouth, and Verizon. The complaint alleges that defendants disclosed plaintiffs' telephone communications records to the Government. The complaint asserts violations of the Communications Act and common law invasion of privacy on behalf of all California-resident subscribers of defendants' whose information has allegedly been disclosed or sold to the Government.
- *Dolberg v. AT&T Corp*, No. CV 06-78-M-DWM (D. Mont., filed May 15, 2006), was filed in the District of Montana against AT&T Corp. and AT&T Inc. The complaint alleges that defendants disclosed plaintiff's telephone communications records to the

Government. The complaint asserts violations of the Electronic Communications Privacy Act on behalf of all subscribers of AT&T since September 2001.

- *Harrington v. AT&T, Inc.*, No. A06CA374-LY (W.D. Tex., filed May 18, 2006), was filed in the Western District of Texas against AT&T Inc. The complaint alleges that AT&T disclosed plaintiff's telephone communications records to the Government. The complaint asserts violations of the Electronic Communications Privacy Act on behalf of all Texas-resident subscribers of defendants' whose information has been disclosed to the Government.
- *Ludman v. AT&T Inc.*, No. 1:06-cv-00917-RBW (D.D.C., filed May 15, 2006), was filed in the District of Columbia against AT&T, Inc. The complaint alleges that AT&T disclosed plaintiff's telephone and internet communications records to the Government. The complaint asserts violations of the Electronic Communications Privacy Act on behalf of all subscribers of AT&T telephone and internet services since September 2001.
- *Mahoney v. AT&T Communications, Inc.*, No. 1:06-cv-00223-T-LDA (D.R.I., filed May 15, 2006), was filed in the District of Rhode Island against AT&T Communications, Inc. The complaint alleges that AT&T disclosed plaintiff's telephone and internet communications records to the Government. The complaint asserts violations of the Electronic Communications Privacy Act on behalf of all subscribers of AT&T's telephone and internet services since September 2001.
- *Schwarz v. AT&T Corp.*, No. 1:06-cv-02680 (N.D. Ill., filed May 15, 2006), was filed in the Northern District of Illinois against AT&T. The complaint alleges that AT&T disclosed plaintiffs' telephone and internet communications records to the Government. The complaint asserts violations of the Electronic Communications Privacy Act and the First and Fourth Amendments on behalf of all subscribers of AT&T's telephone and internet services since September 2001.
- *Souder v. AT&T, Corp.*, No. 06CV1058-DMS AJB (S.D. Cal., filed May 12, 2006), was filed in the Southern District of California against AT&T Corp. and AT&T Inc. The complaint alleges that AT&T disclosed plaintiff's telephone and internet communications records to the Government. The complaint asserts violations of the Electronic Communications Privacy Act on behalf of all subscribers of AT&T's telephone and internet services since September 2001.
- *Trevino v. AT&T Corp.*, No. 2:06-cv-00209 (S.D. Tex., filed May 17, 2006), was filed in the Southern District of Texas against AT&T Corp. and AT&T Inc. The complaint alleges that AT&T disclosed plaintiff's telephone and internet communications records to the Government. The complaint asserts violations of the Electronic Communications Privacy Act on behalf of all subscribers of AT&T's telephone and internet services since September 2001.
- *Terkel v. AT&T Inc.*, No. 06C-2837 (N.D. Ill., filed May 22, 2006) was filed in the Northern District of Illinois against AT&T Inc. The complaint alleges that AT&T disclosed plaintiffs' telephone and internet communications records to the Government. The complaint asserts violations of the Electronic Communications Privacy Act on behalf of all Illinois-resident subscribers of AT&T's electronic and computing services.

- *Phillips v. BellSouth Corp.*, No. 3:06-CV-00469 (D.D.C., filed May 15, 2006), was filed in the District of Columbia against BellSouth Corp. The complaint alleges that BellSouth disclosed plaintiffs' telephone and internet communications records to the Government. The complaint asserts violations of the Electronic Communications Privacy Act on behalf of all subscribers of BellSouth's telephone and internet services since September 2001.
- *Potter v. BellSouth Corp.*, No. 3 06-0469 (M.D. Tenn., filed May 15, 2006), was filed in the Middle District of Tennessee against BellSouth Corp. The complaint alleges that BellSouth disclosed plaintiffs' telephone and internet communications records to the Government. The complaint asserts violations of the Electronic Communications Privacy Act on behalf of all subscribers of BellSouth's remote computing or electronic communication services since September 2001.
- *Hepting v. AT&T Corp.*, No. 06-0672 (N.D. Cal., filed Jan. 31, 2006), like the cases identified above, challenges telecommunications companies' alleged cooperation with Government intelligence collection programs. The *Hepting* complaint involves the alleged disclosure of the *content* of international telephone calls. In *Hepting*, the United States filed a statement of interest, moved to intervene, and filed a motion to dismiss or for summary judgment on the grounds that the "state secrets" privilege bars the prosecution of this civil action.

Argument

I. **THESE ACTIONS ARE APPROPRIATE FOR TRANSFER AND PRETRIAL COORDINATION UNDER 28 U.S.C. § 1407.**

28 U.S.C. § 1407(a) provides that this Panel may transfer for pretrial coordination two or more civil cases upon a determination (a) that the cases "involve[] one or more common questions of fact," (b) that the transfers would further "the convenience of the parties and witnesses," and (c) that the transfers "will promote the just and efficient conduct of [the] actions." *Id.* As explained below, the cases listed in defendants' Schedule of Actions clearly meet these criteria and should be transferred for coordinated pretrial proceedings.

A. **There are Unique Reasons To Centralize These Cases.**

As discussed below, these cases meet all the traditional requirements of Section 1407. But there are also unique and critical aspects of these cases which independently (and strongly) support their pretrial transfer and coordination. These cases are not standard commercial, products liability, or securities actions, but rather involve issues of vital national security and the

handling of classified information. Allowing this litigation to go forward in multiple venues simply increases the likelihood that classified information might inadvertently be compromised. See National Security Agency Act, 50 U.S.C. § 402; *United States v. Reynolds*, 345 U.S. 1, 7-8 (1953); *Ellsberg v. Mitchell*, 709 F.2d 51, 57 (1983), *cert. denied sub nom. Russo v. Mitchell*, 465 U.S. 1038 (1984). Even assuming that each court decides to review the same sensitive evidence *in camera* and *ex parte*, such review still carries grave risks, including the risks associated with transporting classified information to multiple venues across the country. As one court has recognized,

It is not to slight judges, lawyers or anyone else to suggest that [even *in camera*, *ex parte* review] disclosure carries with it serious risk that highly sensitive information may be compromised. In our own chambers, we are ill equipped to provide the kind of security highly sensitive information should have.

Clift v. United States, 597 F.2d 826, 829 (2d Cir. 1979) (quoting *Alfred A. Knopf, Inc. v. Colby*, 509 F.2d 1362, 1369 (4th Cir.), *cert. denied*, 421 U.S. 992 (1975)). These security concerns will be reduced if the litigation is conducted in one forum.

B. These Actions Involve One Or More Common Questions Of Fact.

1. The Cases Involve the Same or Similar Facts and Theories of Recovery.

The actions at issue clearly meet the first requirement of § 1407(a). The factual allegations underlying each of the purported class actions are essentially identical. All of the complaints generally allege that, starting in late 2001, the defendants disclosed records pertaining to plaintiffs' use of telecommunications services to the National Security Agency.⁴ They further

⁴ (See, e.g., *Bissitt Compl.* ¶ 2; *Conner Compl.* ¶ 1; *Driscoll Compl.* ¶¶ 2-5; *Fuller Compl.* ¶¶ 3-6; *Herron Compl.* ¶ 4; *Hines Compl.* ¶¶ 11-12; *Mahoney v. Verizon Compl.* ¶¶ 2-5; *Mahoney v. AT&T Compl.* ¶¶ 2-5; *Marck Compl.* ¶ 6; *Mayer Compl.* ¶¶ 7-8; see also *Dolberg Compl.* ¶¶ 3-6; *Harrington Compl.* ¶ 1; *Ludman Compl.* ¶¶ 2-5; *Phillips Compl.* ¶¶ 2-5; *Potter Compl.* ¶ 7; *Schwarz Compl.* ¶¶ 3-6; *Souder Compl.* ¶¶ 2-5; *Trevino Compl.* ¶¶ 2-4; *Terkel Compl.* ¶ 2.)

allege that the defendants disclosed these records without Plaintiffs' knowledge or consent.⁵ And, at bottom, all of the complaints except *Hepting* purport to be based on the May 11, 2006 *USA Today* article described above. "Common" factual allegations thus exist across these cases.

The claims for relief are also similar. All but one of the complaints (*Conner*) asserts that the defendants violated the Electronic Communications Privacy Act, 18 U.S.C. § 2701, *et seq.*⁶ In fact, many of the complaints are "copycat" putative class actions that are in all material respects identical save for the identity of the named plaintiffs and the district courts in which they were filed. The *Driscoll*, *Fuller*, and *Mahoney* complaints against Verizon, for example, offer virtually identical allegations,⁷ propose the same putative class,⁸ and assert the same causes of action.⁹

The Panel has long recognized that class actions asserting such similar claims based on such similar underlying factual allegations are particularly well suited for coordination pursuant to § 1407. *See, e.g., In re Cooper Tire & Rubber Co. Tires Prods. Liab. Litig.*, No. 1393, 2001 WL 253115 (J.P.M.L. Feb. 23, 2001) (transfer ordered where "[a]ll actions involve allegations relating to Cooper's tire design and its manufacturing process"); *In re St. Jude Med., Inc., Silzone Heart Valves Prods. Liab. Litig.*, Docket No. 1396, 2001 U.S. Dist. LEXIS 5226, at *2-3

⁵ (See *Bissitt* Compl. ¶ 33; *Conner* Compl. ¶ 6; *Driscoll* Compl. ¶¶ 46, 53; *Fuller* Compl. ¶¶ 45, 52; *Herron* Compl. ¶ 4 (disclosure "without proper authorization"); *Hines* Compl. ¶ 12; *Mahoney v. Verizon* Compl. ¶¶ 44, 51; *Mahoney v. AT&T* Compl. ¶¶ 44, 51; *Marck* Compl. ¶ 3; *Mayer* Compl. ¶ 13; *see also Dolberg* Compl. ¶¶ 45, 52; *Harrington* Compl. ¶¶ 3-4; *Ludman* Compl. ¶¶ 44, 51; *Phillips* Compl. ¶¶ 44, 51; *Potter* Compl. ¶¶ 6-7; *Schwarz* Compl. ¶¶ 122-29; *Souder* Compl. ¶¶ 45, 52; *Trevino* Compl. ¶ 54; *Terkel* Compl. ¶ 24.)

⁶ (See *Bissitt* Compl. ¶¶ 29-43; *Driscoll* Compl. ¶¶ 43-56; *Fuller* Compl. ¶¶ 42-55; *Herron* Compl. ¶ 7; *Hines* Compl. ¶¶ 15-17; *Mahoney v. Verizon* Compl. ¶¶ 41-54; *Mayer* Compl. ¶¶ 18-31; *Dolberg* Compl. ¶¶ 42-55; *Harrington* Compl. ¶¶ 26-28; *Ludman* Compl. ¶¶ 41-54; *Mahoney v. AT&T* Compl. ¶¶ 41-54; *Phillips* Compl. ¶¶ 41-54; *Potter* Compl. ¶ 1; *Schwarz* Compl. ¶¶ 119-32; *Souder* Compl. ¶¶ 42-55; *Trevino* Compl. ¶¶ 51-57; *Terkel* Compl. ¶¶ 29-32.)

⁷ (See *Driscoll* Compl. ¶¶ 16-32, *Fuller* Compl. ¶¶ 15-31; *Mahoney v. Verizon* Compl. ¶¶ 14-30; *Mahoney v. AT&T* Compl. ¶¶ 14-30.)

⁸ (See *Driscoll* Compl. ¶ 33, *Fuller* Compl. ¶ 32; *Mahoney v. Verizon* Compl. ¶ 31; *Mahoney v. AT&T* Compl. ¶ 31.)

⁹ (See *Driscoll* Compl. ¶¶ 43-56; *Fuller* Compl. ¶¶ 42-55; *Mahoney v. Verizon* Compl. ¶¶ 41-54; *Mahoney v. AT&T* Compl. ¶¶ 41-54.)

(J.P.M.L. Apr. 18, 2001) (transfer ordered where “[a]ll actions are brought as class actions . . . and arise from the same factual milieu, namely the manufacture and marketing of allegedly defective heart valve and replacement products”); *In re America Online, Inc., Version 5.0 Software Litig.*, Docket No. 1341, 2000 U.S. Dist. LEXIS 13262 (J.P.M.L. June 2, 2000) (transfer ordered where class action plaintiffs alleged that AOL Version 5.0 conflicted with various types of non-AOL software); *In re Gen. Motors Corp. Type III Door Latch Prods. Liab. Litig.*, Docket No. 1266, 1999 U.S. Dist. LEXIS 5075, at *1-2 (J.P.M.L. Apr. 14, 1999) (transfer ordered where “the three actions in this litigation involve common questions of fact concerning allegations that the ‘unmodified Type III door latches’ on certain GM vehicles are defective and prone to failure”); *In re Chrysler Corp. Vehicle Paint Litig.*, Docket No. 1239, 1998 U.S. Dist. LEXIS 15675 (J.P.M.L. October 2, 1998) (transfer ordered where “the actions in this litigation involve common questions of fact concerning allegations by overlapping classes of defects in the paint of certain Chrysler vehicles that result in chipping, peeling and discoloration of the paint finish”).

2. The Cases Seek Certification of Overlapping Nationwide Classes.

The case for transfer and coordination is particularly strong here because plaintiffs seek certification of not merely “parallel” class actions in various states but completely “overlapping” proposed classes purporting to join consumers from coast to coast. Fifteen of the 20 cases propose nationwide class actions on behalf of customers of residential telecommunications services provided by the defendants. Others involve single-state class allegations.¹⁰ Another complaint involves a proposed multi-state class action.¹¹ Still another complaint is ambiguous,

¹⁰ (*Connor* Compl. ¶ 18; *Harrington* Compl. ¶ 17; *Terkel* Compl. ¶ 16.)

¹¹ (*Hines* Compl. ¶ 4.)

but could be read to encompass a request for nationwide class certification.¹² Such overlapping class actions almost by definition satisfy the requirements of § 1407. *See, e.g., In re Jamster Mktg. Litig.*, No. 3:05-1915, 2006 WL 1023460 (J.P.M.L. Apr. 14, 2006) (ordering transfer where “[e]ach action is brought as a class action against overlapping defendants and is predicated on the same factual allegations”); *In re Hydrogen Peroxide Antitrust Litig.*, 374 F. Supp. 2d 1345, 1346 (J.P.M.L. 2005) (finding centralization warranted when “[e]ach of the actions now before the Panel is brought under the Sherman Act to recover for injuries sustained as a result of an alleged conspiracy engaged in by overlapping defendants to fix, raise, maintain, or stabilize prices for hydrogen peroxide and its downstream products sodium perborate and sodium percarbonate”); *In re High Sulfur Content Gasoline Prods. Liab. Litig.*, 344 F. Supp. 2d 755, 756 (finding centralization warranted of five “overlapping putative class actions brought on behalf of purchasers of gasoline that contained high levels of sulfur in May 2004”); *In re Chrysler Corp. Vehicle Paint Litig.*, 1998 U.S. Dist. LEXIS 15675 (transfer ordered where “the actions in this litigation involve common questions of fact concerning allegations by overlapping classes of defects in the paint of certain Chrysler vehicles that result in chipping, peeling and discoloration of the paint finish”). Absent coordination, multiple federal courts will simultaneously be handling the same claims brought by the same classes of plaintiffs against the same defendants.

3. There is No Warrant for Waiting for Additional Filings.

The 20 putative class actions already on file plainly warrant transfer and coordination. This Panel has not hesitated to afford MDL treatment to litigation matters involving as few as two or three class actions to serve the interests and convenience and judicial economy.¹³ This

¹² (Mayer Compl. ¶¶ 1, 33.)

¹³ *See, e.g., In re LifeUSA Holdings, Inc. Annuity Contracts Sales Practices Litig.*, No. 1273, 1999 U.S. Dist. LEXIS 4918 (J.P.M.L. Apr. 7, 1999) (consolidating two actions) *In re the Hartford Sales Practices Litig.*, No. 1204, 1997 U.S. Dist. LEXIS 19671 (J.P.M.L. Dec. 8, 1997) (consolidating two actions); *In re Mountain States Tel. & Tel.*

litigation involves 19 purported class actions filed in the past 12 days. If the pending cases are transferred and coordinated, any later-filed lawsuits could be included as “tag-along” cases in the MDL proceeding. *See In re Gas Meter Antitrust Litig.*, 464 F. Supp. 391 (J.P.M.L. 1979) (major reason for the Panel’s transfer order was the salutary effect of providing a ready forum for the inclusion of expected newly filed actions).

C. Coordination Will Serve The Convenience Of Parties And Witnesses.

Coordination of these actions will also satisfy the second criterion of § 1407(a) – it will serve the “convenience of [the] parties and witnesses.” As discussed in more detail above, the allegations in these cases implicate classified information. Without coordination, that information might have to be transported to multiple venues simply to support *in camera* and *ex parte* review in connection with the Government’s likely intervention and invocation of the state secrets privilege. That would not be a matter of mere inconvenience, but a risk to national security. Further, the pretrial activities in these cases – starting with the likely litigation over the state-secrets privilege – almost certainly will overlap considerably. To the extent pretrial discovery is required, the defendants may be subjected to myriad duplicative discovery demands, and witnesses may be subjected to equally duplicative depositions. Absent coordination, unnecessary burdens will be imposed upon the courts, the parties, and the United States.

By contrast, centralization will avoid those grave risks and wasteful duplicative efforts. Because discovery has not yet been conducted, it can be efficiently coordinate from the start of any MDL proceeding by the transferee court. Transfer would thus “effectuate a significant overall savings of cost and a minimum of inconvenience to all concerned with the pretrial

Co. Employees Benefit Litig., No. 798, 1989 U.S. Dist. LEXIS 13673 (J.P.M.L. Feb. 2, 1989) (consolidating two actions); *In re New Mexico Natural Gas Antitrust Litig.*, 482 F. Supp. 333 (J.P.M.L. 1979) (consolidating three actions); *In re California Armored Car Antitrust Litig.*, 476 F. Supp. 452, 454 (J.P.M.L. 1979) (consolidating three actions); *In re First Nat’l Bank*, 451 F. Supp. 995, 997 (J.P.M.L. 1978) (consolidating two actions); *In re E. Airlines*,

activities.” *In re Cuisinart Food Processor Antitrust Litig.*, 506 F. Supp. 651, 655 (J.P.M.L. 1981).

D. Coordination Will Promote Just And Efficient Conduct Of The Actions.

Coordination of the pending actions will also promote the third Section 1407(a) criterion – the just and efficient conduct of the actions.

1. Coordination Will Prevent Conflicting Pretrial Rulings.

Given the virtually identical factual allegations, theories of recovery, and proposed class definitions, pretrial activities such as motion practice will overlap substantially. As the United States has already explained in the *Hepting* case, a threshold question in this litigation is whether these cases may proceed at all, or whether they should instead be dismissed as a result of the Government’s likely assertion of the “state-secret” privilege. Absent coordinated proceedings, that singular threshold issue involving national security will needlessly be decided by multiple federal judges across the country.

Moreover, additional motions and discovery will overlap considerably, risking inconsistent rulings by different district courts on the same issues. Transfer is thus warranted. *See, e.g., In re Cooper Tire & Rubber Co. Tires Prods. Liab. Litig.*, No. 1393, 2001 WL 253115, at *1 (“Motion practice and relevant discovery will overlap substantially in each action. Centralization under Section 1407 is thus necessary in order to eliminate duplicative discovery, prevent inconsistent pretrial rulings, and conserve the resources of the parties, their counsel and the judiciary.”); *In re St. Jude Med., Inc., Silzone Heart Valves Prods. Liab. Litig.*, Docket No. 1396, 2001 U.S. Dist. LEXIS 5226, at *3 (J.P.M.L. Apr. 18, 2001) (“Centralization under Section 1407 is necessary in order to eliminate duplicative discovery, prevent inconsistent

Inc. Flight Attendant Weight Program Litig., 391 F. Supp. 763 (J.P.M.L. 1975) (consolidating two actions); *In re Cross-Florida Barge Canal Litig.*, 329 F. Supp. 543 (J.P.M.L. 1971) (consolidating two actions).

pretrial rulings (especially with respect to questions of privilege issues, confidentiality issues and class certification), and conserve the resources of the parties, their counsel and the judiciary.”); *In re Am. Online, Inc., Version 5.0 Software Litig.*, Docket No. 1341, 2000 U.S. Dist. LEXIS 13262, at *3-4 (J.P.M.L. June 2, 2000) (to same effect); *In re Gen. Motors Corp. Type III Door Latch Prods. Liab. Litig.*, Docket No. 1266, 1999 U.S. Dist. LEXIS 5075, at *2 (J.P.M.L. Apr. 14, 1999) (to same effect); *In re Chrysler Corp. Vehicle Paint Litig.*, Docket No. 1239, 1998 U.S. Dist. LEXIS 15675, at *2 (J.P.M.L. Oct. 2, 1998) (to same effect).

Plaintiffs in various cases have already begun rattling their sabers by suggesting that they will seek preliminary injunctive relief, raising the specter (absent coordination) that the defendants could possibly be subjected to competing injunctions entered in short order by various federal courts.¹⁴ Coordination is needed to prevent inconsistent injunctive orders. *See In re Operation of the Mo. River Sys. Litig.*, 277 F. Supp. 2d 1378, 1379 (J.P.M.L. 2003) (holding that MDL treatment was necessary to avoid inconsistent pretrial rulings “particularly with respect to requests for preliminary injunctive relief imposing or threatening to impose conflicting standards of conduct”); *In re General Motors Class E Stock Buyout Sec. Litig.*, 696 F. Supp. 1546, 1547 (J.P.M.L. 1988) (“The presence of common questions in *Hart* and MDL-720 is further illustrated by the overlapping injunctive relief sought in both proceedings. Transfer of *Hart* under Section 1407 is thus necessary to avoid duplication of discovery, prevent inconsistent pretrial rulings, and conserve the resources of the parties, their counsel and the judiciary.”)

¹⁴ *Bissit* Compl. Prayer for Relief; *Driscoll* Compl. Request for Relief; *Fuller* Compl. Request for Relief; *Mahoney* Compl. Request for Relief; *Dolberg* Compl. Request for Relief; *Harrington* Compl. ¶ 39; *Ludman* Compl. Request for Relief; *Mahoney v. AT&T* Compl. Request for Relief; *Schwarz* Compl. Prayer for Relief; *Souder* Compl. Request for Relief; *Trevino* Compl. Prayer for Relief; *Terkel* Compl. Prayer for Relief; *Phillips* Compl. Request for Relief; *Hepting* Compl. Prayer for Relief.

2. Transfer Will Facilitate Uniform Class Certification Decisions.

Because the purported class allegations in each of these cases are virtually identical, and the proposed classes overlap in significant respects, the arguments presented both for and against certification will presumably be similar. There is a danger of inconsistent rulings on class certification and other class action-related issues if these cases are not coordinated, not to mention unnecessary duplication of effort by the parties and the courts.

The Panel has “consistently held that transfer of actions under § 1407 is appropriate, if not necessary, where the possibility of inconsistent class determinations exists.” *In re Sugar Indus. Antitrust Litig.*, 395 F. Supp. 1271, 1273 (J.P.M.L. 1975); *see also In re Bridgestone/Firestone, Inc. ATX, ATX II and Wilderness Tires Prods. Liab. Litig.*, 2000 U.S. Dist. LEXIS 15926 (J.P.M.L. Oct. 24, 2000) (“Centralization under Section 1407 is thus necessary in order to . . . prevent inconsistent pretrial rulings (particularly with respect to overlapping class certification requests”); *In re America Online, Inc., Version 5.0 Software Litig.*, 2000 U.S. Dist. LEXIS 13262 (same); *In re Temporomandibular TMJ Implants Prods. Liab. Litig.*, 844 F. Supp. 1553, 1554 (J.P.M.L. 1994) (same); *In re Roadway Express, Inc. Employment Practices Litig.*, 384 F. Supp. 612, 613 (J.P.M.L. 1974) (“the existence of and the need to eliminate [the possibility of inconsistent class determinations] presents a highly persuasive reason favoring transfer under Section 1407”); *In re Plumbing Fixture Cases*, 298 F. Supp. 484, 493 (J.P.M.L. 1968) (transfer necessary to avoid “pretrial chaos in conflicting class action determinations”); *In re Hawaiian Hotel Room Rate Antitrust Litig.*, 438 F. Supp. 935, 936 (J.P.M.L. 1977) (“[s]ection 1407 centralization is especially important to ensure consistent treatment of the class action issues”); *In re Mut. Fund Sales Anti-Trust Litig.*, 361 F. Supp. 638, 639-40 (J.P.M.L. 1973) (“we have frequently held that the possibility for conflicting class

determinations under [Fed. R. Civ. P. 23] is an important factor favoring transfer of all actions to a single district”).

II. THIS PANEL SHOULD TRANSFER THESE ACTIONS TO THE DISTRICT COURT FOR THE DISTRICT OF COLUMBIA.

Verizon respectfully recommends that this Panel transfer these cases to the United States District Court for the District of Columbia. Transfer of these cases there would maximize the benefits of coordination by serving the interests and convenience of the parties and the courts.

First, the District Court for the District of Columbia already has three constituent actions pending before it – more cases than are pending in any other district. Between them, the three cases name as defendants all three principal telecommunications carriers identified in the May 11, 2006 *USA Today* article: Verizon, AT&T, and BellSouth. MDL actions are commonly transferred to a forum where one or more actions is pending. *In re A.H. Robins Co. “Dalkon Shield” Liab. Litig.*, 406 F. Supp. 540, 542 (J.P.M.L. 1975).

Second, the District of Columbia is the preferable forum for transfer because of the district court’s and court of appeals’ extensive experience with national security issues in past cases. It is no overstatement to suggest that both this District and Circuit are, given their proximity to the United States Government, uniquely experienced to handle this kind of case. *See, e.g., Bancoult v. McNamara*, No. 05-5049, 2006 U.S. App. LEXIS 10065 (D.C. Cir. Apr. 21, 2006) (suit under FTCA against the Government for setting up military base on Diego Garcia); *Bennett v. Chertoff*, 425 F.3d 999 (D.C. Cir. 2005) (Title VII suit against Defense Department arising out of termination after employee could not sustain security clearance); *Schneider v. Kissinger*, 412 F.3d 190 (D.C. Cir. 2005) (suit against Henry Kissinger for alleged torture acts committed against deceased Chilean general); *In re Grand Jury Subpoena (Miller)*, 397 F.3d 964 (D.C. Cir. 2005) (New York Times reporter refused to reveal source

notwithstanding Government's insistence that she do so on national security grounds); *ACLU v. FBI*, No. 05-1004, 2006 U.S. Dist. LEXIS 25290 (D.D.C. May 2, 2006) (addressing FOIA request in light of national-security exemption); *Millennium Pipeline Co., L.P. v. Gutierrez*, No. 04-233, 2006 U.S. Dist. LEXIS 14273 (D.D.C. Mar. 31, 2006) (discussing national security issues under Coastal Zone Management Act); *Adem v. Bush*, No. 05-00723, 2006 U.S. Dist. LEXIS 17070 (D.D.C. Mar. 14, 2006) (representation of prisoner at Guantanamo Bay); *AFGE v. Rumsfeld*, No. 05-2183, 2006 U.S. Dist. LEXIS 7068 (D.D.C. Feb. 27, 2006) (addressing national security justification for collective bargaining policy at Department of Defense); *Elec. Privacy Info. Ctr. v. DOJ*, 416 F. Supp. 2d 30 (D.D.C. 2006) (FOIA requests for information about domestic communications surveillance); *Leighton v. CIA*, 412 F. Supp. 2d 30 (D.D.C. 2006) (Privacy Act suit against CIA for publication of facts surrounding plaintiff's stripped security clearance following communication of classified information). Indeed, Judge Walton, to whom the three constituent cases pending in the District of Columbia have been assigned, has specific experience with both the state-secrets privilege and similar national security matters. See *Edmonds v. United States*, 323 F. Supp. 2d 65, (D.D.C. 2004); *United States v. Libby*, Criminal No. 05-394, 2006 U.S. Dist. LEXIS 24911 (D.D.C. May 3, 2006).

Third, although the Government is currently a defendant only in one of these actions, the complaints center on an alleged Government program.¹⁵ Relevant information will likely be located in or near the District of Columbia, yet another reason to transfer the cases there. See *In re Salomon Bros. Treasury Sec. Litig.*, 796 F. Supp. 1537, 1538 (J.P.M.L. 1992) (designating as transferee court the district where the documents and witnesses relating to the defendant's

conduct were located); *In re Air Disaster at Denver*, 486 F. Supp. 241, 243 (J.P.M.L. 1980) (same); *In re Air Crash Disaster at Stapleton International Airport*, 447 F. Supp. 1071, 1073 (J.P.M.L. 1978) (same); *In re U. S. Financial Sec. Litig.*, 375 F. Supp. 1403, 1404 (J.P.M.L. 1978) (same). Further, given the Government's interest in the allegations of these complaints, as well as its actions in the *Hepting* case, it is also likely that the United States will intervene in these cases to protect national security interests. Accordingly, the Justice Department, which has already expressed a strong interest in this matter on behalf of the United States, will be well served by centralization in the District of Columbia.

Fourth, centralizing the cases in the District of Columbia will reduce the considerable logistical burdens associated with protecting classified information. For instance, in the *Hepting* proceeding, the classified affidavits supporting the Government's assertion of the state secret privilege must be flown to San Francisco for the court's review, and then flown back to the District of Columbia immediately after that review, because of the absence of suitable secure facilities in San Francisco. *See* Hearing Transcript, *Hepting*, No. 3:06-CV-0672-VRW, at 32 (D.D.C. May 17, 2006), attached hereto at Tab C. Absent coordination, the same cumbersome procedure might be necessary in a multitude of locations. It is logistically far superior to have any classified information reviewed *in camera* either in chambers or a suitable alternative in the District of Columbia, where secure facilities exist, than in a judicial district hundreds or thousands of miles away from the facilities housing the classified information. These cases involve matters of national security, and there is no warrant for potentially jeopardizing that

¹⁵ (See, e.g., *Bissitt* Compl. ¶ 2; *Driscoll* Compl. ¶¶ 2-5; *Fuller* Compl. ¶¶ 3-6; *Herron* Compl. ¶ 4; *Hines* Compl. ¶¶ 11-12; *Mahoney v. Verizon* Compl. ¶¶ 2-5; *Marck* Compl. ¶ 6; *Mayer* Compl. ¶¶ 7-8; see also *Dolberg* Compl. ¶¶ 3-6; *Harrington* Compl. ¶ 1; *Ludman* Compl. ¶¶ 2-5; *Mahoney v. AT&T* Compl. ¶¶ 2-5; *Phillips* Compl. ¶¶ 2-5; *Potter* Compl. ¶ 7; *Schwarz* Compl. ¶¶ 3-6; *Souder* Compl. ¶¶ 2-5; *Trevino* Compl. ¶¶ 2-4; *Terkel* Compl. ¶ 2.)

security by requiring classified information to be transported from one side of the country to the other.

Fifth, The District of Columbia has the capacity to give an MDL proceeding the necessary time and attention. Of the district courts where these cases have been filed, the District of Columbia had among the fewest pending cases on its docket per judge last year:

Dist.	Pending Cases 2005 (U.S. Rank)
D.R.I.	329 (70)
E.D.N.Y.	622 (11)
S.D.N.Y.	689 (10)
E.D. La.	444 (32)
S.D. Tex.	529 (18)
W.D. Tex.	404 (42)
M.D. Tenn.	391 (48)
N.D. Ill.	360 (59)
D. Mont.	401 (43)
D. Or.	535 (16)
E.D. Cal.	1060 (4)
N.D. Cal.	468 (25)
S.D. Cal.	256 (83)
D.D.C.	309 (76)

Federal Court Management Statistics (2005) at <http://www.uscourts.gov/fcmstat/index.html>
(emphasis added).

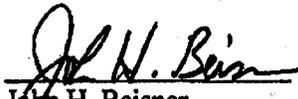
Sixth, the District of Columbia is a convenient forum for most of the parties, including the United States. Verizon and AT&T both maintain a significant corporate presence in the District of Columbia, making Washington D.C. a logical center of gravity for the defendants. Counsel for a number of parties are also present in the District of Columbia. Finally, and as noted above, the United States Government is likely to intervene in these cases, and the District of Columbia is obviously the most convenient forum for it.

Conclusion

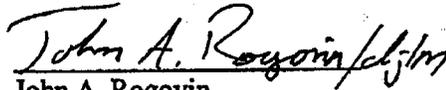
For all the foregoing reasons, the coordination of these overlapping putative class actions would further "the convenience of [the] parties and witnesses and [would] promote the just and efficient conduct of [the] actions." 28 U.S.C. § 1407(a). Therefore, Verizon respectfully requests that this Panel enter an order transferring the actions listed in the accompanying Schedule of Actions to the United States District Court for the District of Columbia.

Dated: May 24, 2006

Respectfully submitted,



John H. Beisner
Brian D. Boyle
Thomas E. Donilon
Matthew M. Shors
O'MELVENY AND MYERS LLP
1625 Eye Street, NW
Washington, DC 20006
(202) 383-5300 (phone)
(202) 383-5414 (fax)



John A. Rogovin
Randolph D. Moss
Samir Jain
Brian Boynton
WILMER CUTLER PICKERING HALE AND
DORR LLP
1875 Pennsylvania Avenue, N.W.
Washington, DC 20006
(202) 663-6000 (phone)
(202) 663-6363 (fax)

Attorneys for Verizon Communications Inc., Verizon Global Networks Inc., and Verizon Northwest Inc.

RECEIVED
CLERK'S OFFICE

2006 MAY 24 P 3 08

JUDICIAL PANEL ON
MULTIDISTRICT
LITIGATION

BEFORE THE JUDICIAL PANEL
ON MULTIDISTRICT LITIGATION

In re NATIONAL SECURITY AGENCY
LITIGATION

MDL Docket No. _____

**VERIZON'S SCHEDULE OF NATIONAL SECURITY AGENCY ACTIONS FOR
TRANSFER AND COORDINATION**

Pursuant to Rule 7.2(a)(ii) of the Rules of Procedure of the Judicial Panel on Multidistrict Litigation, defendants Verizon Communications Inc., Verizon Global Networks Inc., and Verizon Northwest Inc. (collectively "Verizon") provide the following information on the actions that will be affected by their Motion for Transfer and Coordination Pursuant to 28 U.S.C. § 1407:

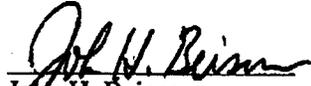
Plaintiffs	Defendants	Division / City	Civil Action No.	Judge Assigned
E.D. Cal.				
Greg Conner; Mark Boulet; Sergio Vasquez; James Bolich; Debra Bolich; Cheryl Scroggins; Melissa Scroggins; M. Diedre Wilten; Stephen M. Kampmann; Lloyd Brown; Claudia Salazar	AT&T; BellSouth; Verizon; Does 1 - 50	Fresno	1:06-at-00225	None assigned yet.
S.D. Cal.				
Shelly D. Souder	AT&T Corp.; AT&T Inc.		06 cv 1058 DMS AJB	The Honorable Dana M. Sabraw
N.D. Cal.				
Tash Hepting; Gregory Hicks; Erik Knutzen	AT&T Corp.; AT&T, Inc.; Does 1 - 20		C 06 0672	The Honorable Vaughn R. Walker
D.D.C.				
David M. Driscoll, Jr.; Anne Brydon Taylor; Cory Brown	Verizon Communications, Inc.		06-cv-00916-RBW	The Honorable Reggie B. Walton
Harold Ludman	AT&T, Inc.		06-cv-00917-RBW	The Honorable Reggie B. Walton
Lawrence Phillips	BellSouth Corporation		06-cv-00918-RBW	The Honorable Reggie B. Walton
N.D. Ill.				
Steven Schwarz; James Joll; Ramon Goggins	AT&T Corp.; AT&T Inc.; Does 1 - 20		1:06-cv-0280	The Honorable Matthew F. Kennelly
Studs Terkel; Barbara Flynn Curie; Diane C. Geraghty; Gary S. Gerson; James D. Montgomery; Quentin Young; American Civil Liberties Union of Illinois	AT&T Inc.		06C 2837	The Honorable James B. Zagel

E.D. La.				
Tina Herron; Brandy Sergi	Verizon Global Networks, Inc.; AT&T Corp; American Telephone and Telegraph Company; BellSouth Communication Systems, LLC; BellSouth Telecommuncations, Inc.		06-2491	The Honorable Jay C. Zainey.
D. Mont.				
Steve Dolberg	AT&T Corp., AT&T, Inc.	Missoula	CV-06-78-M-DWM	The Honorable Donald W. Molloy
Rhea Fuller	Verizon Communications, Inc.; Verizon Wireless, LLC	Missoula	CV-06-77-DWM	The Honorable Donald W. Molloy
E.D.N.Y.				
Edward Marck; Carol Waltuch	Verizon Communications, Inc.; Does 1 - 10		CV-06 2455	The Honorable Joseph F. Bianco
S.D.N.Y.				
Carl J. Mayer; Bruce I. Afran	Verizon Communciations Inc.; National Security Agency; George W. Bush		06 cv 3650	The Honorable Leonard B. Sand
D. Or.				
Darryl Hines	Verizon Northwest, Inc.		CV 06 694	The Honorable Janice M. Stewart

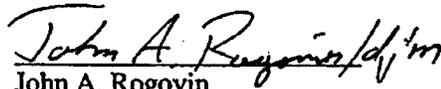
D.R.I.				
Charles F. Bissitt, Sandra Bissitt, George Hayek, III, June Matrumalo, Gerard Thibeault, Arthur Bouchard, Maryann Bouchard, Aldo Caparco, Janice Caparco, Jenna Caparco, Rose Deluca, Nicole Mirabella, Patricia Pothier, Paul Pothier, Marshall Votta, Vincent Matrumalo, Paula Matrumalo, Jennifer Thomas, Christine Douquette, Maryanne Klaczynski	Verizon Communications, Inc., BellSouth Corporation		06-220	The Honorable William E. Smith
Pamela A. Mahoney	AT&T Communications, Inc.		CA 06 223	The Honorable Ernest C. Torres
Pamela A. Mahoney	Verizon Communications, Inc.		CA 06 224	The Honorable William E. Smith
M.D. Tenn.				
Kathryn Potter	BellSouth Corp.		3 06*0469	The Honorable William J. Haynes, Jr.
S.D. Tex.				
Mary J. Trevino	AT&T Corp.; AT&T Inc.	Corpus Christi	2:06-cv- 00209	The Honorable Hayden W. Head, Jr.
W.D. Tex.				
James C. Harrington; Richard A. Grigg; Louis Black; The Austin Chronicle; Michael Kentor	AT&T, Inc.	Austin	A06CA374 LY	The Honorable Earl Leroy Yeakel III

Dated: May 24, 2006

Respectfully submitted,



John H. Beisner
Brian D. Boyle
Thomas E. Donilon
Matthew M. Shors
O'MELVENY AND MYERS LLP
1625 Eye Street, NW
Washington, DC 20006
(202) 383-5300 (phone)
(202) 383-5414 (fax)



John A. Rogovin
Randolph D. Moss
Samir Jain
Brian Boynton
WILMER CUTLER PICKERING HALE AND
DORR LLP
1875 Pennsylvania Avenue, N.W.
Washington, DC 20006
(202) 663-6000 (phone)
(202) 663-6363 (fax)

*Attorneys for Verizon Communications Inc., Verizon Global Networks Inc., and Verizon
Northwest Inc.*

CERTIFICATE OF SERVICE

I, the undersigned, hereby certify that a true and correct copy of Defendants Verizon Communications Inc., Verizon Global Networks Inc., and Verizon Northwest Inc.'s Notice of Filing of Motion for Transfer and Coordination Pursuant to 28 U.S.C. § 1407 (with supporting memorandum and the exhibits thereto) have been delivered via first class mail to the clerk of the following federal district courts in which an action is pending that will be affected by this Motion, on this 24th day of May, 2006:

The Honorable Donald S. Black United States District Court for the Eastern District of California Fresno Division 2500 Tulare St Fresno, CA 93721	The Honorable Dana M. Sabraw United States District Court for the Southern District of California United States Courthouse 940 Front Street San Diego, CA 92101
The Honorable Vaughn R. Walker United States District Court for the Northern District of California United States Courthouse 450 Golden Gate Avenue San Francisco, CA 94102	The Honorable Reggie B. Walton United States District Court for the District of Columbia United States Courthouse 333 Constitution Avenue, N.W. Washington, D.C. 20001-2866
The Honorable Matthew F. Kennelly United States District Court for the Northern District of Illinois Everett McKinley Dirksen Building 20th floor 219 South Dearborn Street Chicago, Illinois 60604	The Honorable James B. Zigel United States District Court for the Northern District of Illinois Everett McKinley Dirksen Building 20th floor 219 South Dearborn Street Chicago, Illinois 60604
The Honorable Jay C. Zainey United States District Court for the Eastern District of Louisiana 500 Poydras Street New Orleans, LA 70130	The Honorable Donald W. Molloy United States District Court for the District of Montana Russell Smith Federal Building 201 East Broadway Post Office Box 7309 Missoula, MT 59801
The Honorable Joseph F. Bianco United States District Court for the Eastern District of New York 225 Cadman Plaza East Brooklyn, NY 11201	The Honorable Leonard B. Sand United States District Court for the Southern District of New York 500 Pearl Street New York, NY 10007

CERTIFICATE OF SERVICE

<p>The Honorable Janice M. Stewart United States District Court for the District of Oregon Mark O. Hatfield U.S. Courthouse 1000 S.W. Third Avenue Portland, OR 97204-2902</p>	<p>The Honorable William E. Smith United States District Court for the District of Rhode Island Federal Building and Courthouse One Exchange Terrace Providence, RI 02903</p>
<p>The Honorable Ernest C. Torres United States District Court for the District of Rhode Island Federal Building and Courthouse One Exchange Terrace Providence, RI 02903</p>	<p>The Honorable William J. Haynes, Jr. United States District Court for the Middle District of Tennessee United States Courthouse 801 Broadway Nashville, TN 37203</p>
<p>The Honorable Hayden W. Head, Jr. United States District Court for the Southern District of Texas 1133 N Shoreline Blvd Corpus Christi, TX 78401</p>	<p>The Honorable Earl Leroy Yeakel III United States District Court for the Western District of Texas U.S. District Clerk's Office 200 West 8th St., Room 130 Austin, Texas 78701</p>

I, the undersigned, certify that a copy of Defendants Verizon Communications Inc., Verizon Global Networks Inc., and Verizon Northwest Inc.'s Motion for Transfer and Coordination Pursuant to 28 U.S.C. § 1407 (with supporting memorandum and the exhibits thereto) has been served via first class mail to the following plaintiff's counsel of record for all of the actions that will be affected by this motion, on this 24th day of May, 2006:

CERTIFICATE OF SERVICE

<p>Michael A. St. Pierre REVENS REVENS & ST. PIERRE, PC 946 Centerville Road Warwick, RI 02886 401-822-2900 (Telephone) 401-826-3246 (Fax) <i>Attorney for Plaintiffs Charles F. Bissitt, Sandra Bissit, George Hayek, III, June Matrumalo, Gerard Thibeault, Arthur Bouchard, Maryann Bouchard, Aldo Caparco, Janice Caparco, Jenna Caparco, Rose Deluca, Nicole Mirabella, Patricia Pothier, Paul Pothier, Marshall Votta, Vincent Matrumalo, Paula Matrumalo, Jennifer Thomas, Christine Douquette, Maryanne Klaczynski</i></p>	<p>Amato A. DeLuca DELUCA & WEIZENBAUM, LTD. 199 North Main Street Providence, RI 02903 401-453-1500 (Telephone) 401-453-1501 (Fax) <i>Attorney for Plaintiffs Charles F. Bissitt, Sandra Bissit, George Hayek, III, June Matrumalo, Gerard Thibeault, Arthur Bouchard, Maryann Bouchard, Aldo Caparco, Janice Caparco, Jenna Caparco, Rose Deluca, Nicole Mirabella, Patricia Pothier, Paul Pothier, Marshall Votta, Vincent Matrumalo, Paula Matrumalo, Jennifer Thomas, Christine Douquette, Maryanne Klaczynski</i></p>
<p>Nicholas "Butch" Wagner Andrew B. Jones Daniel M. Kopfman LAW OFFICE OF WAGNER & JONES 1111 E. Herndon, Suite 317 Fresno, California 93720 559-449-1800 559-449-0749 <i>Attorneys for Plaintiffs Greg Conner; Mark Boulet; Sergio Vasquez; James Bolich; Debra Bolich; Cheryl Scroggins; Melissa Scroggins; M. Diedre Wilten; Stephen M. Kampmann; Lloyd Brown; Claudia Salazar</i></p>	<p>Timothy M. Bechtold William A. Rossbach ROSSBACH HART BECHTOLD, P.C. 401 North Washington P.O. Box 8988 Missoula, Montana 59807 406-543-5156 406-728-8878 <i>Attorneys for Plaintiffs Steve Dolberg; Rhea Fuller</i></p>
<p>Marc R. Stanley Roger L. Mandel Martin Woodward STANLEY, MANDEL & IOLA, LLP 3100 Monticello Avenue, Suite 750 Dallas, TX 75205 Telephone: 214-443-4300 Facsimile: 214-443-0358 <i>Attorneys for Plaintiffs Steve Dolberg; Rhea Fuller</i></p>	<p>Gary E. Mason THE MASON LAW FIRM, P.C. 1225 19th Street, NW Suite 500 Washington, D.C. 20038 Telephone: 202-429-2290 Facsimile: 202-429-2294 <i>Attorney to Plaintiffs Harold Ludman; Pamela A. Mahoney; Lawrence Phillips</i></p>

CERTIFICATE OF SERVICE

<p>Alexander E. Barnett THE MASON LAW FIRM, P.C. One Pennsylvania Plaza Suite 4632 New York, NY 10119 Telephone: 212-362-5770 Facsimile: 917-591-5227 <i>Attorney to Plaintiffs Harold Ludman; Pamela A. Mahoney; Lawrence Phillips</i></p>	<p>Peter N. Wasylyk LAW OFFICES OF PETER N. WASYLYK 1307 Chalkstone Avenue Providence, RI 02908 Telephone: 401-831-7730 Facsimile: 401-861-6064 <i>Attorney to Plaintiffs Harold Ludman; Pamela A. Mahoney; Lawrence Phillips</i></p>
<p>Andrew Kierstead LAW OFFICES OF ANDREW KIERSTEAD 1001 S.W. 5th Ave., Suite 1100 Portland, OR 97204 Telephone: 508-224-6246 Facsimile: 508-224-4356 <i>Attorney to Plaintiffs Harold Ludman; Pamela A. Mahoney; Lawrence Phillips</i></p>	<p>R. James George, Jr. Douglas Brothers GEORGE & BROTHERS, L.L.P. 1100 Norwood Tower 114 W. 7th Street Austin, Texas 78701 Telephone: 512-495-1400 Facsimile: 512-499-0094 <i>Attorneys for Plaintiff James C. Harrington; Richard A. Grigg; Louis Black; The Austin Chronicle; Michael Kentor</i></p>
<p>Cindy Cohn Lee Tien Kurt Opsahl Kevin S. Bankston Corynne McSherry James S. Tyre ELECTRONIC FRONTIER FOUNDATION 454 Shotwell Street San Francisco, CA 94110 Telephone: 415-436-9333 Facsimile: 415-436-9993 <i>Attorneys for Tash Hepting; Gregory Hicks; Erik Knutzen</i></p>	<p>Bert Voorhees Theresa M. Traber TRABER & VOORHEES 128 North Fair Oaks Avenue, Suite 204 Pasadena, CA 91103 Telephone: 626-585-9611 Facsimile: 626-577-7079 <i>Attorneys for Tash Hepting; Gregory Hicks; Erik Knutzen</i></p>
<p>Reed R. Kathrein Shana E. Scarlett LERACH COUGHLIN STOIA GELLER RUDMAN & ROBBINS LLP 100 Pine Street, Suite 2600 San Francisco, CA 94111 Telephone: 415-288-4545 Facsimile: 415-288-4534</p>	<p>Val Patrick Exnicios Amy Fontenot LISKA, EXNICIOS & NUNGESSER One Canal Place, Ste. 2290 365 Canal Street New Orleans, LA 70130 Telephone: 504-410-9611 Facsimile: 504-410-9937 <i>Attorneys for Plaintiffs Tina Herron; Brandy Sergi</i></p>

CERTIFICATE OF SERVICE

<p>Conrad S.P. Williams Joseph G. Jevic III Melanie G. Lagarde ST. MARTIN & WILLIAMS P.O. Box 2017 Houma, Louisiana 70361 Telephone: 985-876-3891 <i>Attorneys for Plaintiffs Tina Herron; Brandy Sergi</i></p>	<p>Anthony Irpino 365 Canal Street, Ste. 2290 New Orleans, LA 70130 504-525-1500 <i>Attorneys for Plaintiffs Tina Herron; Brandy Sergi</i></p>
<p>Christopher A. Slater Michael J. Ross 1850 Umpqua Bank Plaza One S.W. Columbia Street Portland, Oregon 97258 Telephone: 503-227-2024 Facsimile: 503-224-7299 <i>Attorney for Plaintiff Darryl Hines</i></p>	<p>Marc R. Stanley Roger L. Mandel Martin Woodward STANLEY, MANDEL & IOLA, LLP 3100 Monticello Avenue, Suite 750 Dallas, TX 75205 Telephone: 214-443-4300 Facsimile: 214-443-0358 <i>Attorneys to Plaintiff Pamela A. Mahoney</i></p>
<p>Michael C. O'Malley, Esq. SIBEN & SIBEN LLP 90 East Main Street Bay Shore, NY 11706 631-665-3400 <i>Attorney to Plaintiffs Edward Marck; Carol Waltuch</i></p>	<p>Carl J. Mayer 66 Witherspoon Street - Suite 414 Princeton, New Jersey 08542 609-921-0253 <i>Pro se Plaintiff</i></p>
<p>Bruce I. Afran 10 Braeburn Drive Princeton, New Jersey 08540 609-924-2075 <i>Pro se Plaintiff</i></p>	<p>Matthew J. Piers Patrick M. O'Brien Joshua Karsh HUGHES SOCOL PIERS RESNICK & DYM, LTD. Three First National Plaza, Suite 4000 Chicago, Illinois 60602 Telephone: 312-580-0100 Facsimile: 312-580-1994 <i>Attorneys for Plaintiff Kathryn Potter</i></p>
<p>C. David Briley Tennessee PBR 18559 BRILEY LAW GROUP, PLLC 511 Union St., Ste. 1610 Nashville, IN 37219 Telephone: 615-986-2684 Facsimile: 615-986-7869 <i>Attorneys for Plaintiff Kathryn Potter</i></p>	<p>STEVEN E. SCHWARZ 2461 W. Foster Ave., #1W Chicago, IL 60625 <i>Pro se Plaintiff, and attorney for Plaintiffs James Joll; Ramon Goggins</i></p>

CERTIFICATE OF SERVICE

<p>Derek J. Emge EMGE & ASSOCIATES 550 West C. Street, Suite 1600 San Diego, CA 92101 Telephone: 619-595-1400 Facsimile: 619-595-1480 <i>Attorneys for Plaintiff Shelly D. Souder</i></p>	<p>Matthew J. Zevin STANLEY MANDEL & IOLA LLP 550 West C Street, Suite 1600 San Diego, CA 92101 Telephone: 619-235-5306 Facsimile: 815-377-8419 <i>Attorneys for Plaintiff Shelly D. Souder</i></p>
<p>Marc R. Stanley Roger L. Mandel Martin Woodward STANLEY, MANDEL & IOLA, LLP 3100 Monticello Avenue, Suite 750 Dallas, TX 75205 Telephone: 214-443-4300 Facsimile: 214-443-0358 <i>Attorneys for Plaintiff Shelly D. Souder</i></p>	<p>Harvey Grossman Adam Schwartz Wendy Park ROGER BALDWIN FOUNDATION OF ACLU, INC. 180 North Michigan Avenue, Suite 2300 Chicago, Illinois 60601 312-201-9740 <i>Attorneys for Plaintiffs Studs Terkel; Barbara Flynn Curie; Diane C. Geraghty; Gary S. Gerson; James D. Montgomery; Quentin Young; American Civil Liberties Union of Illinois</i></p>
<p>Marc O. Beem Daniel M. Feeney Zachary J. Freeman MILLER SHAKMAN & BEEM LLP 180 North LaSalle Street, Suite 3600 Chicago, Illinois 60601 312-263-3700 <i>Attorneys for Plaintiffs Studs Terkel; Barbara Flynn Curie; Diane C. Geraghty; Gary S. Gerson; James D. Montgomery; Quentin Young; American Civil Liberties Union of Illinois</i></p>	<p>William H. Hooks HOOKS LAW OFFICES PC 29 South LaSalle Street, Suite 333 Chicago, Illinois 60603 312-553-5252 <i>Attorney for Plaintiffs Studs Terkel; Barbara Flynn Curie; Diane C. Geraghty; Gary S. Gerson; James D. Montgomery; Quentin Young; American Civil Liberties Union of Illinois</i></p>
<p>Steven R. Shapiro Ann Beeson AMERICAN CIVIL LIBERTIES UNION FOUNDATION 125 Broad Street, 18th Floor New York, New York 10004 <i>Attorneys for Plaintiffs Studs Terkel; Barbara Flynn Curie; Diane C. Geraghty; Gary S. Gerson; James D. Montgomery; Quentin Young; American Civil Liberties Union of Illinois</i></p>	<p>Robert C. Hilliard 719 S. Shoreline Boulevard, Suite 500 Corpus Christi, Texas 78401 Telephone: 361-882-1612 Telecopier: 361-882-3015 <i>Attorney for Plaintiff Mary J. Trevino</i></p>

CERTIFICATE OF SERVICE

<p>Kevin W. Grillo, HILLIARD & MUÑOZ, L.L.P. 719 S. Shoreline Boulevard, Suite 500 Corpus Christi, Texas 78401 Telephone: 361-882-1612 Facsimile: 361-882-3015 <i>Attorneys for Plaintiff Mary J. Trevino</i></p>	<p>Mikal C. Watts Robert J. Patterson WATTS LAW FIRM, L.L.P. Tower II Building 555 N. Carancahua, Suite 1400 Corpus Christi, Texas 78478 Telephone: 361-887-0500 Facsimile: 361-887-0055 <i>Attorneys for Plaintiff Mary J. Trevino</i></p>
<p>Darrell Barger HARTINE, DACUS, BARGER, DREYER & KERN, LLP One Shoreline Plaza 800 N. Shoreline Blvd., Suite 2000-North Corpus Christi, Texas 78401 Telephone: 361-866-8009 Telecopier: 361-866-8039 <i>Attorney for Plaintiff Mary J. Trevino</i></p>	<p>Edward M. Carstarphen ELLIS, CARSTARPHEN, DOUGHERTY & GOLDENTHAL, P.C. 5847 San Felipe, Suite 1900 Houston, Texas 77057 Telephone: 713-647-6800 Telecopier: 713-647-6884 <i>Attorney for Plaintiff Mary J. Trevino</i></p>

I, the undersigned, certify that a copy of Defendants Verizon Communications Inc., Verizon Global Networks Inc., and Verizon Northwest Inc.'s Motion for Transfer and Coordination Pursuant to 28 U.S.C. § 1407 (with supporting memorandum and the exhibits thereto) has been served via first class mail (and through agreement) to the following defense counsel of record for all of the actions that will be affected by this motion, on this 24th day of May, 2006:

<p>Bradford A. Berenson Sara J. Gourley Susan A. Weber Sidley & Austin LLP 1501 K Street, N.W. Washington, D.C. 20005 (202) 736-8971 (202) 736-8711 <i>Attorney to Defendants AT&T Corp.; AT&T Inc.; AT&T Communications Inc.</i></p>	<p>Jane F. Thorpe Alston & Bird LLP One Atlantic Center 1201 West Peachtree Street Atlanta, GA 30309-3424 (404) 881-7822 (404) 881-7777 <i>Attorney to Defendants BellSouth Corp.</i></p>
--	---

CERTIFICATE OF SERVICE

Matthew Shors
Matthew Shors

EXHIBIT C

1 PILLSBURY WINTHROP SHAW PITTMAN LLP
2 BRUCE A. ERICSON #76342
3 DAVID L. ANDERSON #149604
4 JACOB R. SORENSEN #209134
5 BRIAN J. WONG #226940
6 50 Fremont Street
7 Post Office Box 7880
8 San Francisco, CA 94120-7880
9 Telephone: (415) 983-1000
10 Facsimile: (415) 983-1200
11 Email: bruce.ericson@pillsburylaw.com

12 SIDLEY AUSTIN LLP
13 DAVID W. CARPENTER (admitted *pro hac vice*)
14 DAVID L. LAWSON (admitted *pro hac vice*)
15 BRADFORD A. BERENSON (admitted *pro hac vice*)
16 EDWARD R. McNICHOLAS (admitted *pro hac vice*)
17 1501 K Street, N.W.
18 Washington, D.C. 20005
19 Telephone: (202) 736-8010
20 Facsimile: (202) 736-8711
21 Email: bberenson@sidley.com

22 Attorneys for Defendants
23 AT&T CORP. and AT&T INC.

24 UNITED STATES DISTRICT COURT
25 NORTHERN DISTRICT OF CALIFORNIA
26 SAN FRANCISCO DIVISION

27 TASH HEPTING, GREGORY HICKS,
28 CAROLYN JEWEL and ERIK KNUTZEN
on Behalf of Themselves and All Others
Similarly Situated,

Plaintiffs,

vs.

AT&T CORP., AT&T INC. and DOES 1-20,
inclusive,

Defendants.

No. C-06-0672-VRW

**MOTION OF DEFENDANT
AT&T CORP. TO DISMISS
PLAINTIFFS' AMENDED
COMPLAINT; SUPPORTING
MEMORANDUM**

Date: June 8, 2006
Time: 2 p.m.
Courtroom: 6, 17th Floor
Judge: Hon. Vaughn R. Walker

Filed concurrently:

1. Request for judicial notice
2. Proposed order

1

2 **TABLE OF CONTENTS**

3 NOTICE OF MOTION AND MOTION TO DISMISS..... vi

4 ISSUES TO BE DECIDED..... vi

5 MEMORANDUM OF POINTS AND AUTHORITIES..... 1

6 I. INTRODUCTION AND SUMMARY OF ARGUMENT..... 1

7 II. SUMMARY OF THE CASE..... 2

8 A. Background..... 2

9 B. Standards for deciding this motion..... 4

10 III. ARGUMENT..... 4

11 A. THE FAC FAILS TO PLEAD THE ABSENCE OF IMMUNITY

12 FROM SUIT..... 4

13 1. The FAC fails to plead the absence of absolute statutory

14 immunity..... 5

15 a. Numerous statutes provide telecommunications

16 carriers absolute immunity for assisting governmental

17 activities..... 5

18 b. Plaintiffs have the burden of pleading facts sufficient

19 to avoid these immunities..... 7

20 c. Plaintiffs fail to meet their pleading burden and are

21 relying on extreme and erroneous legal theories..... 10

22 2. The FAC fails to plead the absence of absolute common-law

23 immunity..... 13

24 3. The FAC establishes AT&T's qualified immunity as a matter

25 of law..... 15

26 B. PLAINTIFFS LACK STANDING..... 19

27 1. Plaintiffs have not sufficiently alleged injury-in-fact..... 20

28 2. Plaintiffs' dissatisfaction with government policy does not

give them standing..... 22

3. Plaintiffs fail to allege concrete injuries to their statutory

interests..... 24

IV. CONCLUSION..... 255

1 **TABLE OF AUTHORITIES**

2 **CASES**

3 *Allen v. Wright*,
4 468 U.S. 737 (1984) 19, 23

5 *Baker v. Carr*,
6 369 U.S. 186 (1962) 24

7 *Balistreri v. Pacifica Police Department*,
8 901 F.2d 696 (9th Cir. 1990) 4

9 *Berry v. Funk*,
10 146 F.3d 1003 (D.C. Cir. 1998) 16

11 *Blake v. Wright*,
12 179 F.3d 1003 (6th Cir. 1999) 16

13 *Cahill v. Liberty Mutual Insurance Co.*,
14 80 F.3d 336 (9th Cir. 1996) 4

15 *Calloway v. Boro of Glassboro*,
16 89 F. Supp. 2d 543 (D.N.J. 2000) 17

17 *City of Los Angeles v. Lyons*,
18 461 U.S. 95 (1983) 23

19 *Clegg v. Cult Awareness Network*,
20 18 F.3d 752 (9th Cir. 1994) 4

21 *Collins v. Jordan*,
22 110 F.3d 1363 (9th Cir. 1996) 18

23 *Conley v. Gibson*,
24 355 U.S. 41 (1957) 4

25 *Craska v. New York Telegraph Co.*,
26 239 F. Supp. 932 (N.D.N.Y. 1965) 14

27 *Crawford-El v. Britton*,
28 523 U.S. 574 (1998) 10, 11

Donohoe v. Duling,
465 F.2d 196 (4th Cir. 1972) 22

Electronic Privacy Information Center, et al. v. Department of Justice,
Civil Action No. 06-00096 (HHK) 1

Flast v. Cohen,
392 U.S. 83 (1968) 20

Fowler v. Southern Bell Telegraph & Telegraph Co.,
343 F.2d 150 (5th Cir. 1965) 14

1 *Halkin v. Helms*,
690 F.2d 977 (D.C. Cir. 1982)..... 21

2

3 *Halperin v. Kissinger*,
424 F. Supp. 838 (D.D.C. 1976),
4 *rev'd on other grounds*, 606 F.2d 1192 (D.C. Cir.1979) 14, 15

5 *Harlow v. Fitzgerald*,
457 U.S. 800 (1982)..... 16

6 *Hodgers-Durgin v. de la Vina*,
199 F.3d 1037 (9th Cir. 1999)..... 19

7

8 *Hunter v. Bryant*,
502 U.S. 224 (1991) 16

9 *In re Sealed Case*,
310 F.3d 717 (FISA Ct. Rev. 2002) 12, 18

10

11 *In re VeriFone Sec. Litigation*,
11 F.3d 865 (9th Cir. 1993)..... 4

12 *In re World War II Era Japanese Forced Labor Litigation*,
164 F. Supp. 2d 1160 (N.D. Cal. 2001)..... 23, 24

13

14 *Jacobson v. Rose*,
592 F.2d 515 (9th Cir. 1978)..... 12, 20

15 *Kokonnen v. Guardian Life Insurance Co. of America*,
511 U.S. 375 (1994) 4

16

17 *Laird v. Tatum*,
408 U.S. 1 (1972) 22, 23

18 *Lujan v. Defenders of Wildlife*,
504 U.S. 555 (1992) 19, 21, 23

19

20 *Mejia v. City of New York*,
119 F. Supp. 2d 232 (E.D.N.Y. 2000)..... 17

21 *O'Shea v. Littleton*,
414 U.S. 488 (1974) 19, 23, 24

22

23 *Raines v. Byrd*,
521 U.S. 811 (1997) 19

24 *Richardson v. McKnight*,
521 U.S. 399 (1997) 16, 17

25

26 *Rush v. FDIC*,
747 F. Supp. 575 (N.D. Cal. 1990)..... 16

27 *Schlesinger v. Reservists Committee to Stop the War*,
418 U.S. 208 (1974) 23

28

1 *Siegert v. Gilley*,
500 U.S. 226 (1991) 11

2

3 *Smith v. Nixon*,
606 F.2d 1183 (D.C. Cir. 1979)..... 13

4 *Sprewell v. Golden State Warriors*,
266 F.3d 979 (9th Cir. 2001)..... 4

5

6 *Tapley v. Collins*,
211 F.3d 1210 (11th Cir. 2000) 13, 16

7 *Tenet v. Doe*,
544 U.S. 1, 125 S. Ct. 1230 (2004) 9, 10

8

9 *Thompson v. Dulaney*,
970 F.2d 741 (10th Cir. 1992)..... 8

10 *Totten v. United States*,
92 U.S. 105 (1876)..... 9

11

12 *United Presbyterian Church v. Reagan*,
738 F.2d 1375 (D.C. Cir. 1984)..... 21, 22

13 *United States v. Goldstein*,
532 F.2d 1305 (9th Cir. 1976)..... 9

14

15 *United States v. Reynolds*,
345 U.S. 1 (1953) 9

16 *United States v. SCRAP*,
412 U.S. 669 (1973) 24

17

18 *United States v. Texas*,
507 U.S. 529 (1993)..... 13

19 *United States v. United States Dist. Court (Keith)*,
407 U.S. 297 (1972) 18

20

21 *Valley Forge Christian College v. Americans United for Separation of Church and*
State, Inc.,
454 U.S. 464 (1982) 19, 20, 23

22

23 *Vernon v. City of Los Angeles*,
27 F.3d 1385 (9th Cir. 1994)..... 22

24 *Warren v. Fox Family Worldwide, Inc.*,
328 F.3d 1136 (9th Cir. 2003)..... 4, 11

25

26 *Warth v. Seldin*,
422 U.S. 490 (1975) 19

27 *White v. Lee*,
227 F.3d 1214 (9th Cir. 2000)..... 4

28

1 *Williams v. Poulos*,
11 F.3d 271 (1st Cir. 1993) 7, 8

2

3

4

STATUTES AND OTHER AUTHORITY

5 18 U.S.C. § 798(a)(3) 10

6 18 U.S.C. § 2511 passim

7 18 U.S.C. § 2520 7, 8, 12

8 18 U.S.C. § 2702 6, 9

9 18 U.S.C. § 2703 5, 6, 9, 10, 12

10 18 U.S.C. § 3124(d) 6

11 47 U.S.C. § 605 6, 8, 9

12 50 U.S.C. § 1801 24

13 50 U.S.C. § 1805(i) 6

14 50 U.S.C. § 1809 24

15 50 U.S.C. § 1810 24

16 Cal. Bus. & Prof. Code §17200 25

17 Cal. Bus. & Prof. Code §17204 25

18 Federal Rule of Civil Procedure Rule 12(b)(1) vi, 4

19 Federal Rule of Civil Procedure Rule 12(b)(6) vi, 4

20 Senate Report No. 99-541 (1986) 8

21 Senate Report No. 95-604 (1978) 12

22 Terrorist Surveillance Act of 2006, S. 2455, 109th Cong., 2d Sess. 24

23

24

25

26

27

28

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

NOTICE OF MOTION AND MOTION TO DISMISS

TO ALL PARTIES AND THEIR COUNSEL OF RECORD:

PLEASE TAKE NOTICE that on Thursday, June 8, 2006, at 2:00 p.m., before the Honorable Vaughn R. Walker, United States District Chief Judge, in Courtroom 6, 17th Floor, 450 Golden Gate Avenue, San Francisco, California, defendant **AT&T CORP.** (“AT&T”) will move and hereby does move, pursuant to Rules 12(b)(1) and 12(b)(6) of the Federal Rules of Civil Procedure, to dismiss the Amended Complaint for Damages, Declaratory and Injunctive Relief (Dkt. 8, referred to hereafter as the “Amended Complaint” or the “FAC”) filed by plaintiffs Tash Hepting, Gregory Hicks, Carolyn Jewel and Erik Knutzen (collectively, “plaintiffs”) on February 22, 2006.

This motion is made on the grounds that plaintiffs have failed to meet their burden to plead that defendants lack statutory and common law immunity from suit and that plaintiffs do not have standing to pursue this lawsuit.

This motion is based on this notice of motion and motion, the memorandum that follows, the request for judicial notice filed herewith, the administrative motion filed herewith, all pleadings and records on file in this action, and any other arguments and evidence presented to this Court at or before the hearing on this motion.

ISSUES TO BE DECIDED

1. On the facts as alleged by the plaintiffs, have plaintiffs met their burden to negate the statutory and common law immunities applicable to telecommunications providers that are requested and authorized by the government to lend assistance to government surveillance activities?

2. Do the named plaintiffs have standing to challenge alleged government surveillance activities if their complaint does not allege facts—as opposed to unsupported belief—suggesting that they have been or will be the targets of such surveillance?

1 **MEMORANDUM OF POINTS AND AUTHORITIES**

2 **I. INTRODUCTION AND SUMMARY OF ARGUMENT.**

3 This lawsuit arises out of a disagreement with the federal government's national
4 security policies. Through this lawsuit, the Plaintiffs seek to challenge intelligence
5 activities allegedly carried out by the National Security Agency ("NSA") at the direction of
6 the President, as part of the government's effort to prevent terrorist attacks by al Qaeda and
7 other associated groups. Plaintiffs believe these activities to be unlawful, allege that AT&T
8 is assisting the NSA with those activities, and seek through this lawsuit to hold AT&T
9 liable for its alleged assistance. Whatever the truth of plaintiffs' allegations or the merits of
10 the underlying dispute over the lawfulness of the NSA surveillance activities acknowledged
11 by the President (hereinafter "the Terrorist Surveillance Program" or "Program"), this case
12 has been brought by the wrong plaintiffs and it names the wrong defendants. The real
13 dispute is between any actual targets of the Program and the government.¹ It cannot
14 involve telecommunications carriers (such as AT&T) who are alleged only to have acted in
15 accord with requests for assistance from the highest levels of the government in sensitive
16 matters of national security. And the dispute does not involve average AT&T customers
17 (such as plaintiffs) with no perceptible connection to al Qaeda or international terrorism.

18 Yet rather than seeking to vindicate their position through the political process,
19 plaintiffs have sued AT&T for allegedly providing the government with access to its
20 facilities, even though they do not allege that AT&T acted independently or for any reasons

21 _____
22 ¹ There are numerous other cases pending around the country that challenge the Program
23 directly, either through complaints filed by public interest groups or in the context of
24 criminal cases or asset-blocking actions in which terrorism suspects have suffered
25 concrete adverse consequences due to governmental enforcement actions. *See, e.g.,*
26 *American Civil Liberties Union et al. v. NSA et al.*, Civ. 06-10204 (E.D. Mich.); *Center*
27 *for Constitutional Rights v. Bush et al.*, Civ. 06-313 (S.D.N.Y.); *Electronic Privacy*
28 *Information Center, et al. v. Department of Justice*, Civ. No. 06-00096 (HHK) (D.D.C.);
Al-Haramain Islamic Foundation, Inc., et al. v. George W. Bush, et al., CV-06-274-MO
(D. Ore.); *United States v. al-Timimi*, No. 1:04cr385 (E.D. Va.); *United States v. Aref*,
Crim. No. 04-CR-402 (N.D.N.Y.); *United States v. Albanna, et al.*, Crim. No. 02-CR-
255-S (W.D.N.Y.); *United States v. Hayat, et al.*, Crim. No. S-05-240-GEB (E.D. Cal.).
Copies of select related complaints and other filings are attached to defendants' request
for judicial notice, filed herewith ("RFJN") as Exs. A through I.

1 of its own. On the contrary, plaintiffs allege that AT&T acted at all times at the direction
2 and with the approval of the United States government. *See, e.g.*, FAC ¶ 82. If these
3 allegations were true, it is the government and not AT&T that would be obliged to answer
4 for the lawfulness of the challenged intelligence activities: both Congress and the courts
5 have conferred blanket immunity from suit on providers of communications services who
6 respond to apparently lawful requests for national security assistance from the federal
7 government. We are aware of no case in which a telecommunications carrier – even when
8 known to be involved in such activities – has ever been held liable for allowing or assisting
9 government-directed surveillance. As a result, whether or not it had any role in the
10 Program, AT&T is entitled to immediate dismissal.

11 Moreover, Plaintiffs do not allege any fact suggesting that they themselves have
12 suffered any known, concrete harm from the Terrorist Surveillance Program. Indeed, their
13 allegations expressly place them *outside* the category of targets of the Program, making the
14 likelihood that they have suffered any sort of injury from the Program even lower than the
15 likelihood that would apply to any other American who occasionally makes international
16 calls or surfs the Internet. They thus lack Article III standing. Their disagreement with the
17 government’s surveillance activities may be passionate and sincerely felt, but a passionate
18 and sincere disagreement with governmental policy is not enough to confer standing.

19 **II. SUMMARY OF THE CASE.**

20 **A. Background.**

21 Plaintiffs allege that AT&T provides the NSA with access to its telecommunications
22 facilities and databases as part of an electronic surveillance program authorized directly by
23 the President. *See* FAC ¶¶ 3-6.² Plaintiffs claim that “at all relevant times, the government
24 instigated, directed and/or tacitly approved all of the . . . acts of AT&T Corp.” *Id.* ¶ 82.
25 Plaintiffs do not allege that AT&T carried out any actual electronic surveillance; rather, the

26
27 ² As it must, AT&T accepts plaintiffs’ allegations as true solely for purposes of this
28 motion, and nothing herein should be construed as confirmation by AT&T of any
involvement in the Program or other classified activities.

1 gravamen of the complaint is that AT&T allegedly provided access to databases and
2 telecommunications facilities that enabled the government to do so. *Id.* ¶ 6 (“AT&T Corp.
3 has opened its key telecommunications facilities and databases to direct access by the NSA
4 and/or other government agencies . . .”); *see also id.* ¶¶ 38, 41-42, 46, 51, 61.

5 Plaintiffs base their allegations on newspaper reports of the classified Terrorist
6 Surveillance Program that the President has stated he authorized after September 11, 2001
7 and later reauthorized more than 30 times. FAC ¶¶ 3, 32-33. But plaintiffs’ reading of the
8 newspapers is selective. They refer to public statements of the President and the Attorney
9 General, *see id.* ¶¶ 33-35, but they omit the Attorney General’s description of two key
10 characteristics of the Terrorist Surveillance Program: first, it intercepts the contents of
11 communications where “one party to the communication is outside the United States”—in
12 other words, international communications; second, it intercepts the contents of
13 communications only if the government has “a reasonable basis to conclude that one party
14 to the communication is a member of al Qaeda, affiliated with al Qaeda, or a member of an
15 organization affiliated with al Qaeda, or working in support of al Qaeda.”³

16 Plaintiffs purport to bring this case on behalf of a massive, nationwide class of all
17 individuals who are or were subscribers to AT&T’s services at any time after September
18 2001, and a subclass of California residents. FAC ¶¶ 65-68. But their putative classes
19 expressly exclude the targets of the program described by the Attorney General—any
20 “foreign powers . . . or agents of foreign powers . . . , including without limitation anyone
21 who knowingly engages in sabotage or international terrorism, or activities in preparation
22 therefore.” *Id.* ¶ 70 (citations omitted). Plaintiffs do not allege that they themselves
23 communicate with anyone who might be affiliated with al Qaeda.

24

25

26 ³ Press Briefing by Attorney General Alberto Gonzales and General Michael Hayden,
27 Principal Deputy Director for National Intelligence, *available at* [http://www.whitehouse.
28 gov/news/releases/2005/12/20051219-1.html](http://www.whitehouse.gov/news/releases/2005/12/20051219-1.html) (Dec. 19, 2005) (statement of Attorney
General Gonzales), attached as RFJN Ex. J and also as Attachment 2 to Plaintiff’s request
for judicial notice (Dkt. 20).

1 **B. Standards for deciding this motion.**

2 This motion is made under Rule 12(b)(1) and Rule 12(b)(6). Under Rule 12(b)(6), a
3 case is properly dismissed when the plaintiff can prove no set of facts that would entitle him
4 or her to relief. *Conley v. Gibson*, 355 U.S. 41, 45-46, 78 S. Ct. 99 (1957); *Cahill v. Liberty*
5 *Mut. Ins. Co.*, 80 F.3d 336, 338 (9th Cir. 1996). The court must consider whether,
6 assuming the truth of the complaint's factual allegations, the plaintiff has stated a claim for
7 relief. Dismissal can be based "on the lack of a cognizable legal theory or the absence of
8 sufficient facts alleged under a cognizable legal theory." *Balistreri v. Pacifica Police*
9 *Dep't*, 901 F.2d 696, 699 (9th Cir. 1990). Only allegations of fact are taken as true under
10 Rule 12(b)(6). "Conclusory allegations of law and unwarranted inferences are insufficient
11 to defeat a motion to dismiss for failure to state a claim." *In re VeriFone Sec. Litig.*,
12 11 F.3d 865, 868 (9th Cir. 1993); *Clegg v. Cult Awareness Network*, 18 F.3d 752, 754-55
13 (9th Cir. 1994); *Sprewell v. Golden State Warriors*, 266 F.3d 979, 988 (9th Cir. 2001).

14 Under Rule 12(b)(1), it is presumed that the court lacks jurisdiction, and the plaintiff
15 bears the burden of establishing subject matter jurisdiction. *Kokonnen v. Guardian Life Ins.*
16 *Co.*, 511 U.S. 375, 377, 114 S. Ct. 1673 (1994). Absent jurisdiction, the court must dismiss
17 the case. When a Rule 12(b)(1) motion attacks the court's jurisdiction as a matter of fact,
18 the court is not limited to the allegations of the complaint and may consider extrinsic
19 evidence, including matters of public record. *Warren v. Fox Family Worldwide, Inc.*,
20 328 F.3d 1136, 1139 (9th Cir. 2003); *White v. Lee*, 227 F.3d 1214, 1242 (9th Cir. 2000).

21 **III. ARGUMENT.**

22 **A. THE FAC FAILS TO PLEAD THE ABSENCE OF IMMUNITY FROM SUIT.**

23 Both Congress and the courts have recognized an overriding policy interest in
24 having telecommunications carriers cooperate with government requests for national
25 security or foreign intelligence assistance, leaving the defense of substantive challenges to
26 such activity to the government or the political process. For this reason, carriers who
27 respond to apparently lawful requests for assistance from the federal government enjoy
28 statutory and common-law immunity from suit. The FAC does not allege that AT&T

1 engaged in any surveillance of its own or for its own reasons, or undertook any action
2 without the direction or approval of the federal government; in fact, it affirmatively alleges
3 the opposite. *See* FAC ¶¶ 82-84. Thus, even assuming *arguendo* the truth of plaintiffs'
4 allegations, plaintiffs have failed to negate the statutory and common-law immunities that
5 protect carriers such as AT&T from suit, and AT&T is entitled to immediate dismissal.
6 Plaintiffs ultimately rest their complaint on an extreme legal theory that is simply wrong.

7 **1. The FAC fails to plead the absence of absolute statutory immunity.**

8 **a. Numerous statutes provide telecommunications carriers absolute**
9 **immunity for assisting governmental activities.**

10 In numerous places in the United States Code, Congress has made clear that where
11 the government authorizes a communications provider to cooperate with governmental
12 surveillance, that provider is immune from suit. The FAC alleges only that AT&T acted as
13 an agent of, and at the direction of, the government, and that the Program was authorized
14 and repeatedly reauthorized by the President. FAC ¶¶ 3-6, 82-85. Thus, whatever one's
15 views of the Program, assuming for the sake of argument that the allegations of the FAC
16 were true, it could not be challenged by suing AT&T.

17 Both 18 U.S.C. § 2511(2)(a)(ii) and 18 U.S.C. § 2703(e) provide absolute immunity
18 from any and all claims arising out of the surveillance activities alleged in the FAC:

19 *Notwithstanding any other law*, providers of wire or
20 electronic communication service, their officers, employees
21 and agents . . . are authorized to provide information,
22 facilities, or technical assistance to persons authorized by law
23 to intercept wire, oral, or electronic communications or to
24 conduct electronic surveillance as defined in section 101 of
25 [FISA]. . . if such provider, its officers, employees, or
26 agents, . . . has been provided with

27 (B) a certification in writing by a person specified in
28 section 2518 (7) of this title or the Attorney General of the
United States that no warrant or court order is required by
law, that all statutory requirements have been met, and that
the specified assistance is required

1 18 U.S.C. § 2511(2)(a)(ii) (emphasis added). Immunity under this provision is absolute:
2 “No cause of action shall lie in any court against any provider of wire or electronic
3 communication service, its officer, employees, or agents, . . . for providing information,
4 facilities, or assistance in accordance with the terms of a . . . certification under this
5 chapter.” *Id.* (emphasis supplied).

6 In like fashion, the ECPA confers absolute immunity on communication providers
7 acting with government authorization:

8 *No cause of action shall lie in any court against any provider*
9 *of wire and electronic communication service, its officers,*
10 *employees, agents, or other specified persons providing*
11 *information, facilities, or assistance in accordance with the*
12 *terms of a . . . statutory authorization, or certification under*
13 *this chapter.*

14 18 U.S.C. § 2703(e) (emphasis added).⁴

15 Together, these provisions confer absolute immunity on communications carriers
16 authorized to assist the government in foreign intelligence surveillance. This immunity
17 ensures that intelligence matters will not be aired in the nation’s courts and eliminates the
18 risk that courts of general jurisdiction will issue orders that might impede the government’s
19 ability to obtain intelligence that may be critical to protecting the country against foreign
20 attack. This immunity also ensures that the government can obtain prompt cooperation
21 from communications providers in meeting national security needs, without the chilling
22 effect of potential civil liability. Providers will almost always lack the factual information
23 necessary to evaluate the necessity or propriety of classified intelligence activities; to assure
24 that they do not have to argue or equivocate when the government asks for help, the risk of

24 ⁴ “[T]his chapter” includes 18 U.S.C. § 2702(b)(2), which cross references 18 U.S.C.
25 § 2511(2)(a)(ii), making clear that the immunity extends to certifications for foreign
26 intelligence surveillance under the latter provision. FISA and the Communications Act
27 both contain analogous immunity provisions. *See* 50 U.S.C. § 1805(i) (immunity for
28 providing assistance “in accordance with a court order or request for emergency
assistance under this chapter”); 47 U.S.C. § 605(a)(6) (immunity for providing
investigative assistance “on demand of other lawful authority”); *see also* 18 U.S.C.
§ 3124(d) (immunity for compliance with pen register requests).

1 liability for wrongful foreign intelligence surveillance activities is placed not on the
2 providers but on the government.

3 **b. Plaintiffs have the burden of pleading facts sufficient to avoid**
4 **these immunities.**

5 Congress gave plaintiffs the burden to plead specific facts demonstrating the
6 absence of immunity when suing a communications provider for allegedly assisting the
7 government with surveillance. By providing that “no cause of action shall lie” against
8 providers who have acted in accord with governmental authorizations, Congress made the
9 absence of immunity an element of plaintiffs’ claims – and not an affirmative defense.

10 That is reflected in the provisions of the Act that provide for causes of action. For
11 example, the FAC’s Count III alleges interception and disclosure of communications in
12 violation of 18 U.S.C. § 2511 under a right of action created by 18 U.S.C. § 2520(a). In
13 defining that right of action, Congress provided that:

14 *Except as provided in section 2511(2)(a)(ii), any person*
15 *whose wire, oral, or electronic communication is intercepted,*
16 *disclosed or intentionally used in violation of this chapter*
17 *may in a civil action recover from the person or entity, other*
than the United States, which engaged in that violation such
relief as may be appropriate.

18 *Id.* (emphasis added). The highlighted language makes clear that, to state a claim for a
19 violation of § 2520(a), a plaintiff must allege facts showing that the immunities of
20 § 2511(2)(a)(ii) do not apply. None of the other statutory exceptions to § 2511—*e.g.*, the
21 switchboard-operator exception (§ 2511(2)(a)(i)), the FCC exception (§ 2511(2)(b)), or the
22 consent exception (§ 2511(2)(c))—is similarly referenced in § 2520’s definition of the
23 cause of action. Only the absence of an immunity under § 2511(2)(a)(ii) was singled out by
24 Congress as a necessary element of any claim under § 2520.⁵ *Cf. Williams v. Poulos,*

25

26 ⁵ 18 U.S.C. § 2520(d) further provides that it “is a complete defense against any civil or
27 criminal action brought under this chapter or *any other law*” (emphasis added) that the
28 provider acted in “good faith reliance” on “a statutory authorization” or based on a “good
faith determination” that the required authorization under § 2511(2)(a)(ii) existed. The
(continued...)

1 11 F.3d 271, 284 (1st Cir. 1993) (plaintiff's burden of proof in an action under 18 U.S.C.
2 § 2520 includes demonstrating that § 2511 immunity does not apply); *Thompson v.*
3 *Dulaney*, 970 F.2d 744, 749 (10th Cir. 1992) (same). Because § 2511(2)(a)(ii) immunity
4 precludes liability on any theory in any court, the same rule necessarily applies to all causes
5 of action based on the same alleged conduct.

6 The legislative history of ECPA confirms that Congress intended providers to be
7 relieved of the burdens of litigation when complying with government requests for
8 assistance. With respect to § 2520(a), authorizing civil suits against violators of § 2511,
9 Senate Report No. 99-541 (1986) states:

10 Proposed subsection 2520(a) of title 18 authorizes the
11 commencement of a civil suit. There is one exception. A
12 civil action will not lie where the requirements of section
13 2511(2)(a)(ii) of title 18 are met. With regard to that
exception, the Committee intends that the following
procedural standards will apply:

14 (1) The *complaint must allege* that a wire or electronic
15 communications service provider (or one of its employees):
16 (a) disclosed the existence of a wiretap; (b) acted without a
17 facially valid court order or certification; (c) acted beyond the
18 scope of a court order or certification or (d) acted on bad
faith. . . . *If the complaint fails to make any of these*
allegations, the defendant can move to dismiss the complaint
for failure to state a claim upon which relief can be granted.

19 *Id.* at 26 (reprinted in 1986 U.S.C.C.A.N. 3555, 3580) (emphasis supplied). In addition, the
20 Report explains that "in the absence of [a criminal] prosecution and conviction [for the acts
21 complained of], it is the *plaintiff's burden* to establish that the requirements of [section
22 2520] are met." *Id.* at 27. (emphasis supplied). The specifics of other statutes at issue
23 reinforce this understanding.⁶

24
25 (... continued)
26 designation of "good faith reliance" as a "defense" indicates that § 2511(2)(a)(ii)
delineates something that is more than a defense – *i.e.*, an affirmative requirement that
any § 2520(a) claim must allege that § 2511(2)(a)(ii) does not apply.

27 ⁶ For example, 47 U.S.C. § 605 (FAC Count IV) expressly includes the absence of
28 § 2511(2)(a)(ii) immunity as an element of plaintiffs' claim. *Cf. United States v.*
(continued...)

1 Well-established judicial precedents and principles of national security law
2 reinforce the wisdom and necessity of these congressionally-mandated pleading rules.
3 Courts considering suits involving secret military or intelligence programs have long held
4 that the question of immunity should be decided at the outset. In *Tenet v. Doe*, 544 U.S. 1,
5 125 S. Ct. 1230 (2004), for example, the Supreme Court recently reaffirmed a line of
6 precedent stretching back more than a century barring lawsuits against the government
7 based on secret espionage agreements. This rule was announced in *Totten v. United States*,
8 92 U.S. (2 Otto) 105 (1876), which barred an action by a man who claimed that President
9 Lincoln had hired him at \$200 a month to spy on the “insurrectionary States.” *Totten*,
10 92 U.S. at 105-06. The rule holds that “where success [in litigation] depends upon the
11 existence of [a] secret espionage relationship,” *Tenet*, 125 S. Ct. at 1236, a lawsuit must be
12 “dismissed on the pleadings without ever reaching the question of evidence,” *id.* at 1237
13 (quoting *United States v. Reynolds*, 345 U.S. 1, 11 n.26 (1953) (emphasis omitted)). The
14 *Tenet* Court specifically noted that the “absolute protection” afforded by the *Totten*
15 immunity was “designed not merely to defeat the asserted claims, but to preclude judicial
16 inquiry.” *Tenet*, 125 S. Ct. at 1235 n.4, 1237. As such, national security-related immunity
17 “represents the sort of threshold question we have recognized may be resolved before
18 addressing jurisdiction.” *Id.* at 1235 n.4 (internal quotation marks omitted).

19 The statutory immunities provided to telecommunications carriers in this context
20 are, like the rules of dismissal in *Totten* and *Tenet* – and for like reasons – designed to

21 (... continued)

22 *Goldstein*, 532 F.2d 1305, 1312 (9th Cir. 1976) (“The language of the amendment to
23 § 605 providing that “except as authorized by chapter 119, title 18, United States
24 Code . . . no person may disclose certain wire communications, is a clear manifestation
25 of Congress’ intent that § 605 shall not limit § 2511 investigations.”). And 18 U.S.C.
26 § 2702(a)(1), (2), and (3) (FAC Counts V and VI) are subject to the same requirement.
27 Section 2702 states that “[e]xcept as provided in subsection (b),” it is illegal for persons
28 or entities providing either an “electronic communication service” or a “remote
computing service” to make certain disclosures. Subsection (b)(2) makes lawful the
disclosure of the contents of communications “as otherwise authorized in section 2517,
2511(2)(a), or 2703 of this title” (emphasis added). Because the statutory prohibition
itself expressly incorporates and permits any disclosure authorized by § 2511(2)(a), these
statutory causes of action, too, make the absence of § 2511(2)(a)(ii) immunity an element
of the claim and part of plaintiffs’ pleading burden.

1 provide “absolute protection” from such claims. *Id.* at 1236-37. Sections 2711(2)(a)(ii)
2 and 2703(3) both specify that “[n]o cause of action shall lie in any court” if a provider is
3 acting pursuant to governmental authorization. This powerful language assures
4 communications providers that cooperation with the government will not subject them to
5 the burdens of litigation. Where parties are entitled to immunity from suit, “there is a
6 strong public interest in protecting [them] from the costs associated with the defense of
7 damages actions”—an interest best served by dismissing questionable lawsuits
8 expeditiously. *Crawford-El v. Britton*, 523 U.S. 574, 596, 118 S. Ct. 1584 (1998).

9 Immunities such as these are “designed not merely to defeat the asserted claims, but
10 to preclude judicial inquiry.” *Tenet*, 125 S. Ct. at 1235 n.4. That makes particular sense
11 where, as here, if plaintiffs’ allegations were correct, defendants would not be able to
12 mount a factual defense without violating legal prohibitions on disclosure of classified
13 information pertaining to surveillance. *See, e.g.*, 18 U.S.C. § 798(a)(3) (criminalizing
14 disclosure of classified information “concerning the communication intelligence activities
15 of the United States”); 18 U.S.C. § 2511(2)(a)(ii) (forbidding disclosure of “any
16 interception or surveillance” or the “device” used to accomplish it pursuant to government
17 authorized programs). Unless suits making allegations like those in this case (whether true
18 or false) could be dismissed on immunity grounds at the pleading stage, it would be
19 impossible to respect the imperative to “preclude judicial inquiry” into sensitive matters
20 involving the sources and methods of gathering foreign intelligence that Congress and the
21 Executive have concluded must be kept confidential.

22 **c. Plaintiffs fail to meet their pleading burden and are relying on**
23 **extreme and erroneous legal theories.**

24 Plaintiffs fail to meet their burden of alleging specific facts that negate the
25 applicability of statutory immunity. Plaintiffs allege no facts suggesting that, even
26 assuming AT&T engaged in the conduct alleged, AT&T lacked government authorization
27
28

1 under § 2511(2)(a)(ii).⁷ Nor could they: the facts necessary to make (or refute) such an
2 allegation – even assuming they existed – would be completely unavailable to plaintiffs and
3 impossible for either party ever to bring into court.

4 But the flaw in the FAC is even deeper: its allegations, even if true, affirmatively
5 tend to suggest immunity. The gravamen of the FAC is that AT&T allegedly complied
6 with requests to assist in a foreign intelligence program that had been authorized at the
7 highest levels of government. FAC ¶¶ 84-85. Plaintiffs assert that the President himself
8 authorized the Program more than 30 times, *see* FAC ¶ 33, and the Attorney General
9 himself has personally defended it. Most pertinently, plaintiffs expressly allege that “the
10 government instigated, directed and/or tacitly approved all of the . . . acts of AT&T Corp.,”
11 FAC ¶ 82, and that “AT&T Corp. acted as an instrument or agent of the government,” *id.*
12 ¶ 85. This, by its terms, is an allegation that AT&T acted in accord with governmental
13 authorization. There is no suggestion in the FAC that, if AT&T acted, it did so on its own,
14 for its own purposes, or outside the governmental authorization plaintiffs allege.

15 Plaintiffs have elsewhere admitted these points. *See* Pl. Mem. in Support of Mot.
16 for Prelim. Inj. at 19-21. In their injunction papers, they acknowledge that the relevant
17 federal statutes preclude suits against carriers when those carriers receive certain
18 governmental authorizations. Yet here, too, plaintiffs do *not* contend that such
19 authorizations were not provided to AT&T in connection with its alleged assistance.
20 Rather, plaintiffs’ arguments assume that governmental authorizations *were* provided to
21 AT&T, and then go on to defend their complaint under an extreme legal theory that is
22 simply wrong.

23

24 ⁷ The conclusory allegation that AT&T’s actions were “without lawful authorization,” FAC
25 ¶ 81, cannot meet this burden. In this setting, “a ‘firm application of the Federal Rules of
26 Civil Procedure’ is fully warranted,” including but not limited to “insist[ing] that the
27 plaintiff ‘put forward specific nonconclusory factual allegations’ . . . in order to survive a
28 prediscovery motion for dismissal or summary judgment.” *Crawford-El*, 523 U.S. at 598
(*quoting* *Siegert v. Gilley*, 500 U.S. 226, 236 (1991) (Kennedy, J., concurring)). In any
event, FAC ¶ 81 states a legal conclusion that need not be accepted as true on a motion to
dismiss. *Warren*, 328 F.3d at 1139, 1141 n.5.

1 In particular, their legal theory is that, although § 2511(2)(a)(ii) and § 2703(e)
2 categorically provide that “no cause of action lies” against a telecommunications carrier
3 who has acted in accord with governmental authorization, these provisions somehow do not
4 mean what they say. Rather, plaintiffs contend that immunity exists only where
5 authorization has been issued in one of the four circumstances in which FISA specifically
6 authorizes warrantless surveillance and that none of these conditions exists here. This
7 contention is wrong. If Congress had intended to narrow the immunity to those four
8 situations, it would have said so. Congress did not do so because it recognized that where
9 the Attorney General or other responsible officials have authorized surveillance in sensitive
10 areas of national security, it cannot be the province of telecommunications carriers to
11 second-guess them, especially without having the facts to do so.⁸

12 The legal authorities that plaintiffs cite are inapposite. Plaintiffs rely on *Jacobson v.*
13 *Rose*, 592 F.2d 515 (9th Cir. 1978), but that was a case in which the telephone company
14 had *not* acted in accord with a governmental authorization and in which it did not enjoy the
15 absolute immunity of § 2511(2)(a). The Court thus addressed the issue whether the
16 company could rely on the separate good faith immunity conferred by 18 U.S.C. § 2520.
17 Here, by contrast, the issue is absolute statutory immunity, and plaintiffs’ failure to plead its
18 inapplicability cannot be cured by their legal argument that the Program falls outside the
19 four categories of warrantless surveillance authorized by the FISA statute. Even if that
20 were true, it would be a potential legal problem only for the government; it does not affect

21

22 ⁸ To support their attempt to rewrite the immunity provisions of the statutes, plaintiffs refer
23 to the provision of FISA that states that its procedures are the exclusive means of
24 conducting certain surveillance and interceptions. 18 U.S.C. § 2511(f). But this
25 argument ignores that, when FISA was enacted, Congress clearly understood that there
26 were significant areas of warrantless foreign intelligence surveillance the President would
27 continue to direct solely pursuant to his inherent constitutional authority. S. Rep. No. 95-
28 604 at 64 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3904, 3965 ((FISA “does not deal with
international signals intelligence activities as currently engaged in by the National
Security Agency and electronic surveillance conducted outside the United States”). Even
after the passage of FISA, the courts have recognized the President’s continuing
constitutional authority in this area, *See, e.g., In re Sealed Case*, 310 F.3d 717, 742
(FISA Ct. Rev. 2002).

1 the immunity of telecommunications providers under § 2511(2)(a).

2 In short, whatever the merits of the current national debate over the legal authority
3 for the Program, plaintiffs are here alleging only that AT&T acted pursuant to
4 governmental authorization. As such, their allegations are insufficient to permit this lawsuit
5 to go forward in light of the clear statutory immunities enacted by Congress.

6 **2. The FAC fails to plead the absence of absolute common-law immunity.**

7 Not only the Congress but also the courts have long recognized the importance of
8 insulating against suit telecommunications carriers that cooperate with foreign intelligence
9 or law enforcement investigations conducted by the government. The statutory immunities
10 described above were enacted against a backdrop of strong common-law immunities.
11 These common-law immunities too require dismissal of this lawsuit.

12 Statutes in derogation of the common law “are to be read with a presumption
13 favoring the retention of long-established and familiar principles, except when a statutory
14 purpose to the contrary is evident.” *United States v. Texas*, 507 U.S. 529, 534 (1993)
15 (internal quotation marks omitted). The statutory immunities evince no congressional
16 purpose to displace, rather than supplement, the common law. *See, e.g., Tapley v. Collins*,
17 211 F.3d 1210, 1216 (11th Cir. 2000) (“[t]he Federal Wiretap Act lacks the specific,
18 unequivocal language necessary to abrogate the qualified immunity defense”). On the
19 contrary, the statutes and their legislative history bespeak a strong policy consistent with the
20 policies that inspired the common-law immunities.

21 The common-law immunities grew out of a recognition that telecommunications
22 carriers should not be subject to civil liability for cooperating with government officials
23 conducting surveillance activities. That is true whether or not the surveillance was lawful,
24 so long as the government officials requesting cooperation assured the carrier that it was.

25 *Smith v. Nixon*, 606 F.2d 1183, 1191 (D.C. Cir. 1979), illustrates the point. Hedrick
26 Smith, a reporter for *The New York Times*, sued President Nixon, Henry Kissinger and
27 others, including the Chesapeake & Potomac Telephone Company (“C&P”), for tapping his
28 telephone; the taps were part of an investigation by the White House “plumbers” of

1 suspected leaks. The D.C. Circuit reversed the dismissal of claims against the government
2 officials but affirmed the dismissal of claims against C&P, which had installed the wiretap
3 at the request of government officials acting without a warrant. The court rejected the
4 Smiths' claims against C&P out of hand, adopting the district court's reasoning that the
5 telephone company's "limited technical role in the surveillance as well as its reasonable
6 expectation of legality cannot give rise to liability for any statutory or constitutional
7 violation." *Id.* at 1191 (quoting *Smith v. Nixon*, 449 F. Supp. 324, 326 (D.D.C. 1978)); *see*
8 *also id.* (noting that "the telephone company did not initiate the surveillance"). The
9 reasoning derived from the district court's earlier decision in *Halperin v. Kissinger*, 424 F.
10 Supp. 838, 846 (D.D.C. 1976), *rev'd on other grounds*, 606 F.2d 1192 (D.C. Cir. 1979),
11 where the court rejected similar claims against a telephone company arising out of the same
12 surveillance program. The court relied on the fact that the telephone company "played no
13 part in selecting any wiretap suspects or in determining the length of time the surveillance
14 should remain," and that it "overheard none of plaintiffs' conversations and was not
15 informed of the nature or outcome of the investigation." *Id.*

16 This common-law immunity reflects the fact that carriers merely facilitate
17 government-conducted surveillance (rather than engage in surveillance themselves) and
18 would be reluctant to cooperate with the government if they could be sued for doing so.
19 "[T]o deny the [sovereign] privilege to those who assist federal officers would conflict with
20 the underlying policy of the privilege itself: to remove inhibitions against the fearless,
21 vigorous, and effective administration of policies of government." *Fowler v. Southern Bell*
22 *Tel. & Tel. Co.*, 343 F.2d 150, 157 (5th Cir. 1965) (recognizing defense to civil liability for
23 telecommunications carrier); *see also Craska v. New York Tel. Co.*, 239 F. Supp. 932, 936
24 (N.D.N.Y. 1965) (recognizing defense based on "the common sense analysis that must be
25 made of the undisputed minor part the defendant company played in this situation").

26 The FAC describes a classic situation for applying the immunity recognized in
27 *Smith* and *Halperin*. The FAC alleges that AT&T merely had a limited, technical role in
28 facilitating *the government's* surveillance pursuant to a program "the government had

1 instituted” FAC ¶ 3. The core allegation against AT&T is that it “opened its key
2 telecommunications facilities and databases to direct access *by the NSA and/or other*
3 *government agencies*, intercepting and disclosing *to the government* the contents of its
4 customers’ communications as well as detailed communications records.” FAC ¶ 6
5 (emphasis added); *id.* ¶¶ 42-47 (alleging that AT&T has and is providing “the government”
6 with access to transmitted communications through the use of interception devices such as
7 pen registers); *id.* at ¶¶ 48-64; (alleging that AT&T has and is providing “the government”
8 with access to databases containing stored communications records). This is exactly the
9 sort of alleged activity that federal courts found non-actionable in *Smith and Halperin*:
10 taking actions, at the government’s direction, that merely allow government surveillance to
11 be conducted through the carrier’s facilities. The FAC does *not* allege that AT&T selected
12 the targets of the government’s surveillance, determined how long the surveillance would
13 last, overheard conversations, or was told of the nature or outcome of the government’s
14 investigation. Accordingly, the FAC’s allegations against AT&T, even assuming they were
15 true, fall squarely within the immunity recognized by *Smith and Halperin*.

16 The FAC also demonstrates that, even assuming the actions alleged, AT&T would
17 have had a “reasonable expectation” that they were authorized. It alleges that “[t]he
18 President has stated that he authorized the Program in 2001, that he has reauthorized the
19 Program more than 30 times since its inception, and that he intends to continue doing so.”
20 FAC ¶ 33. It alleges that “the government instigated, directed and/or tacitly approved all of
21 the above-described acts of AT&T Corp.” and that “AT&T Corp. had at all relevant times a
22 primary or significant intent to assist or purpose of assisting the government in carrying out
23 the Program and/or other government investigations.” FAC ¶¶ 82, 84; *see also id.* ¶¶ 94, 95
24 (alleging that AT&T’s actions were “under color of law”). The FAC thus alleges the type
25 of cooperation that the common-law immunity is designed to protect and encourage.

26 **3. The FAC establishes AT&T’s qualified immunity as a matter of law.**

27 Even if the plaintiffs had not failed to plead the required absence of the absolute
28 immunity afforded by statute and common law, AT&T would, on the facts as alleged in the

1 FAC, be entitled to qualified immunity as a matter of law.⁹ Federal courts have recognized
2 that qualified immunity is available in addition to statutory immunity under the ECPA. *See*
3 *Tapley*, 211 F.3d at 1216 (“[t]he Federal Wiretap Act lacks the specific, unequivocal
4 language necessary to abrogate the qualified immunity defense”); *Blake v. Wright*, 179 F.3d
5 1003, 1011-13 (6th Cir. 1999).¹⁰ Under the doctrine of qualified immunity, “government
6 officials performing discretionary functions generally are shielded from liability for civil
7 damages insofar as their conduct does not violate clearly established statutory or
8 constitutional rights of which a reasonable person would have known.” *Harlow v.*
9 *Fitzgerald*, 457 U.S. 800, 818, 102 S. Ct. 2727 (1982).

10 Qualified immunity also is available to private parties alleged to have assisted the
11 government in performing traditional governmental functions. The availability of
12 immunity for private parties is determined by analyzing two issues: (1) whether there is “a
13 historical tradition of immunity for private parties carrying out” the functions at issue; and
14 (2) “[w]hether the immunity doctrine’s purposes warrant immunity” for the private parties.
15 *Richardson v. McKnight*, 521 U.S. 399, 407, 117 S. Ct. 2100 (1997) (emphasis in original).
16 These factors both confirm that qualified immunity is available to AT&T here.

17 *First*, federal courts have recognized a common-law immunity from suit that applies
18 to telecommunications carriers that cooperate with government officials conducting
19 warrantless surveillance. *See* page 13 above.

21 _____
22 ⁹ Qualified immunity can be established as a matter of law on a motion to dismiss. *E.g.*,
23 *Rush v. FDIC*, 747 F. Supp. 575, 579-80 (N.D. Cal. 1990). The Supreme Court
24 “repeatedly ha[s] stressed the importance of resolving [qualified] immunity questions at
25 the earliest possible stage in litigation.” *Hunter v. Bryant*, 502 U.S. 224, 227, 112 S. Ct.
26 534 (1991).

27 ¹⁰ *But see Berry v. Funk*, 146 F.3d 1003, 1013-14 (D.C. Cir. 1998) (qualified immunity not
28 available for ECPA claims). The courts in *Tapley* and *Blake* declined to follow *Berry*
because they correctly concluded that it made no sense to “infer that Congress meant to
abolish in the Federal Wiretap Act that extra layer of protection qualified immunity
provides for public officials simply because it included an extra statutory defense
available to everyone.” *Tapley*, 211 F.3d at 1216; *see also Blake*, 179 F.3d at 1012. In
addition, the *Berry* court did not address the principle that qualified immunity can only be
abolished by specific and unequivocal statutory language. *See Tapley*, 211 F.3d at 1216.

1 *Second*, the purposes of qualified immunity are served by affording AT&T
2 immunity on the facts alleged here. Those purposes are: (1) to protect “government’s
3 ability to perform its traditional functions by providing immunity where necessary to
4 preserve the ability of government officials to serve the public good”; (2) “to ensure that
5 talented candidates [are] not deterred by the threat of damages suits from entering public
6 service”; and (3) to protect “the public from unwarranted timidity on the part of public
7 officials” by minimizing the threat of civil liability. *Richardson*, 521 U.S. at 408 (internal
8 quotation marks and citations omitted). Here, even assuming AT&T engaged in the
9 conduct alleged by the plaintiffs, all of these purposes strongly support qualified immunity
10 for AT&T. Conducting surveillance to preserve national security is a traditional
11 governmental function of the highest importance. In an electronic era, such surveillance
12 may require the facilities of private companies that control critical telecommunications
13 infrastructure. Yet carriers would be reluctant to furnish the required assistance if they
14 were exposed to civil liability while the government officials actually ordering the
15 surveillance were cloaked with qualified immunity. It would make little sense to protect
16 the principal but not his agent.¹¹

17
18

19 ¹¹ *Richardson* presented the question whether prison guards employed by a private prison
20 management firm could assert qualified immunity to a section 1983 suit brought by
21 prisoners who alleged that the guards had injured them. The Supreme Court denied
22 immunity, concluding that there is no tradition of immunity for private prison guards and
23 that the private prison managers were “systematically organized” to assume a major
24 governmental function, “for profit” and “in competition with other firms.” *Richardson*,
25 521 U.S. at 405-07, 408-13. In marked contrast, AT&T is part of an industry traditionally
26 immune from liability for assisting the government. Moreover, AT&T is not in the
27 business of surveillance and does not aspire to perform traditional government functions
28 such as espionage. Finally, unlike the private prison guards, AT&T is alleged to be
“serving as an adjunct to government in an essential governmental activity” and “acting
under close official supervision”—the precise context in which the Court suggested that
qualified immunity may be available to private parties. *Id.* at 409, 413. AT&T’s alleged
situation is far closer to that of the citizen who helps law enforcement officials, a situation
in which the federal courts have held that qualified immunity can be available to private
parties. *See Mejia v. City of New York*, 119 F. Supp. 2d 232, 268 (E.D.N.Y. 2000)
(citizen assisting in making an arrest); *Calloway v. Boro of Glassboro*, 89 F. Supp. 2d
543, 557 n.21 (D.N.J. 2000) (sign language interpreter during a police interrogation).

1 Where qualified immunity is available, a two-part analysis determines whether a
2 defendant is entitled to it. The court must determine: (1) “whether the plaintiff has alleged
3 a violation of a right that is clearly established”; and (2) “whether, under the facts alleged, a
4 reasonable official could have believed that his conduct was lawful.” *Collins v. Jordan*,
5 110 F.3d 1363, 1369 (9th Cir. 1996).

6 Under the first prong of the analysis, AT&T’s alleged conduct does not violate any
7 clearly established constitutional or statutory right. If the past several months’ public
8 debate, congressional debate, and legal argumentation over the Program demonstrates
9 anything, it is that the legality of the Program is the subject of reasonable disagreement
10 among well-intentioned and capable lawyers. Indeed, the Supreme Court has specifically
11 reserved the question whether the President has inherent constitutional authority to engage
12 in warrantless foreign intelligence surveillance, see *United States v. United States District*
13 *Court (Keith)*, 407 U.S. 297, 308, 321-22 & n.20 (1972), and the courts of appeals have
14 unanimously held, even after the passage of FISA, that he does. See, e.g., *In re Sealed*
15 *Case*, 310 F.3d at 742 (collecting cases). As such, even if AT&T’s alleged conduct could
16 be directly equated with that of the government – which it cannot – AT&T’s alleged
17 conduct could not amount to “a violation of a right that is clearly established.” *Id.*

18 Second, nothing alleged in the FAC suggests that AT&T’s alleged conduct was
19 carried out in bad faith, *i.e.*, that it did not reasonably believe that any alleged conduct was
20 lawful. The FAC alleges that the President authorized and reauthorized the government
21 surveillance program, that “the government instigated, directed and/or tacitly approved” all
22 of AT&T’s alleged actions, and that AT&T “had at all relevant times a primary or
23 significant intent to assist or purpose of assisting the government in carrying out the
24 Program and/or other government investigations.” *Id.* ¶¶ 33, 82, 84. These allegations
25 demonstrate that, even if AT&T had done what the FAC alleges, it would have had a
26 reasonable belief in the legality of its alleged conduct. Therefore, AT&T is entitled to
27 qualified immunity from suit as a matter of law.

28

1 **B. PLAINTIFFS LACK STANDING.**

2 Under Article III of the Constitution, federal courts have the power to adjudicate
3 only actual “cases” and “controversies.” “The several doctrines that have grown up to
4 elaborate that requirement are founded in concern about the proper—and properly
5 limited—role of the courts in a democratic society,” and “[t]he Art. III doctrine that
6 requires a litigant to have ‘standing’ to invoke the power of a federal court is perhaps the
7 most important of these doctrines.” *Allen v. Wright*, 468 U.S. 737, 750, 104 S. Ct. 3315
8 (1984) (citations omitted).

9 Plaintiffs must establish both constitutional and prudential standing. To establish
10 constitutional standing, plaintiffs must demonstrate (among other things) that they suffered
11 “an injury in fact” that is “concrete and particularized” and “actual or imminent.” *Lujan v.*
12 *Defenders of Wildlife*, 504 U.S. 555, 560-61, 112 S. Ct. 2130 (1992). In the context of a
13 class action, the named plaintiffs “must allege and show that they personally have been
14 injured, not that injury has been suffered by other, unidentified members of the class to
15 which they belong and which they purport to represent.” *Warth v. Seldin*, 422 U.S. 490,
16 502 (1975); *see also O’Shea v. Littleton*, 414 U.S. 488, 494 (1974) (unless named plaintiffs
17 have standing individually, “none may seek relief on behalf of himself or any other member
18 of the class”); *Hodgers-Durgin v. de la Vina*, 199 F.3d 1037, 1045 (9th Cir. 1999) (en banc)
19 (“Any injury unnamed members of this proposed class may have suffered is simply
20 irrelevant . . .”). To establish prudential standing, plaintiffs also must show that their
21 situation differs from that of the public generally. *See Valley Forge Christian College v.*
22 *Americans United for Separation of Church and State, Inc.*, 454 U.S. 464, 474-75, 102 S.
23 Ct. 752 (1982). The standing inquiry must be “especially rigorous” where, as here,
24 “reaching the merits of the dispute would force [a court] to decide whether an action taken
25 by one of the other two branches of the Federal Government was unconstitutional.”
26 *Raines v. Byrd*, 521 U.S. 811, 819-20 (1997).

27

28

1 **1. Plaintiffs have not sufficiently alleged injury-in-fact.**

2 The standing requirement “focuses on the party seeking to get his complaint before
3 a federal court and not on the issues he wishes to have adjudicated.” *Valley Forge*
4 *Christian College*, 454 U.S. at 484 (quoting *Flast v. Cohen*, 392 U.S. 83, 99, 88 S. Ct. 1942
5 (1968)). Thus, the named plaintiffs’ first task is to allege facts showing that *they* have
6 suffered injury in fact. This they have failed to do.

7 In relation to both the Program and the related “data-mining” allegations, the FAC
8 alleges in wholly conclusory terms that plaintiffs’ communications have been or will be
9 “disclosed” to the government, or that AT&T has provided some form of “access” to
10 various databases or datastreams to the government. *See, e.g.*, FAC ¶ 52 (“On information
11 and belief, AT&T Corp. has disclosed and is currently disclosing to the government records
12 concerning communications to which Plaintiffs and class members were a party”); *id.* ¶ 61
13 (“On information and belief, AT&T Corp. has provided the government with direct access
14 to the contents” of various databases that include generic categories information pertaining
15 to plaintiffs); *see also id.* ¶¶ 6, 63, 64, 81, 97, 103, 105, 107, 113, 121, 128, 141. But the
16 FAC alleges only that plaintiffs are (or were) AT&T customers who on occasion make
17 international telephone calls or surf the Internet. FAC ¶¶ 13-16. No allegation suggests
18 that plaintiffs ever communicated with terrorists or with al Qaeda—or gave the government
19 reason to think they had. Indeed, the FAC expressly excludes from the class plaintiffs
20 purport to represent “anyone who knowingly engages in sabotage or international terrorism,
21 or activities that are in preparation therefore.” *Id.* ¶ 70. Absent some concrete allegation
22 that the government monitored their communications or records, all plaintiffs really have is
23 a suggestion that AT&T provided a means by which the government *could have done so*
24 had it wished. This is anything but injury-in-fact.¹²

25

26 ¹² In their injunction papers, plaintiffs implicitly acknowledge that they cannot allege that
27 any “human beings personally read or listen to the acquired communications” but claim it
28 does not matter. Pl. Mem. in Support of Motion for Prelim. Inj. at 17. That is incorrect.
None of the cases cited by plaintiffs is a standing case; all pertain only to the substantive
(continued...)

1 To establish standing, a complaint's allegations must be *factual*. See *Lujan*,
2 504 U.S. at 561. Unsupported conclusions and unwarranted inferences will not suffice.
3 Plaintiffs assert a belief that their communications have somehow been divulged to the
4 government, but they allege no specific facts suggesting that government agents might have
5 targeted them or their communications. The FAC is thus far weaker than other complaints
6 filed by plaintiffs who, while failing to establish standing, at least could muster facts
7 suggesting a governmental interest in their activities.

8 In *United Presbyterian Church v. Reagan*, 738 F.2d 1375, 1380-81 (D.C. Cir.
9 1984), for example, the plaintiffs included a number of stalwarts of the Vietnam antiwar
10 movement and the civil rights movement, such as the former Stokeley Carmichael. *Id.* at
11 1381 n.2. They alleged that they had been or currently were subject to unlawful
12 surveillance, frequently traveled abroad, and were particularly likely to be found to be
13 agents of foreign powers. *Id.* at 1380. Nonetheless, the D.C. Circuit, in an opinion by then-
14 Judge Scalia, held that these activists could not establish standing to challenge Executive
15 Order No. 12333, entitled "United States Intelligence Activities," because they could not
16 show they were subject to surveillance conducted under that Order. Similarly, in *Halkin v.*
17 *Helms*, 690 F.2d 977 (D.C. Cir. 1982), the plaintiffs were antiwar activists who claimed that
18 their communications had been intercepted. *Id.* at 981 n.3. Because they failed to provide
19 factual support for this claim, however, the court held that they lacked standing to challenge
20 government intelligence-gathering activities, including the CIA's "Operation CHAOS."
21 The sole difference between the FAC and these complaints (beyond the fact that the
22 plaintiffs there were noted activists) is that the plaintiffs here use the magic words "on

23 (... continued)

24 scope of liability where plaintiffs' own communications had undoubtedly been monitored
25 and standing was clear. In *Jacobson v. Rose*, 592 F.2d 515 (9th Cir. 1978), for example,
26 the plaintiffs were individuals whose communications had actually been monitored by
27 government agents; class action status was denied, and the district court limited the
28 plaintiffs to those whose conversations had allegedly been overheard. See *id.* at 518.
Nonetheless, the Ninth Circuit reversed a verdict against the phone company. Although
the court said that "the victim's privacy is violated, regardless of which particular
individuals actually listen to the tapes," *id.*, it never suggested that standing exists where
there is no allegation that *anyone* has listened.

1 information and belief” to allege that AT&T has intercepted and disclosed their
2 communications to the government. But that is legally insufficient.

3 Nor can plaintiffs establish standing through the common tactic of alleging that the
4 Program (or AT&T’s alleged involvement) has “chilled” constitutionally-protected
5 activities. Although plaintiffs do not allege “chill” in the FAC, their preliminary injunction
6 papers suggest that at least named-plaintiff Jewel asserts a “chill” on her speech. *See Pl.*
7 *Mem. in Support of Mot. for Prelim. Inj.* at 25-26. This is precisely the kind of abstract
8 injury that the federal courts have consistently held is insufficient to create standing to
9 challenge a government surveillance program. In *Laird v. Tatum*, 408 U.S. 1, 13-15, 92 S.
10 Ct. 2318 (1972), the plaintiffs were held not to have standing to challenge the Army’s
11 domestic surveillance of peaceful, civilian activity based on alleged “chill” because
12 “[a]llegations of a subjective ‘chill’ are not an adequate substitute for a claim of specific
13 present objective harm or a threat of specific future harm.” *Id.* at 13-14. As the D.C.
14 Circuit explained, “[a]ll of the Supreme Court cases employing the concept of ‘chilling
15 effect’ involve situations in which the plaintiff has unquestionably suffered some concrete
16 harm (past or immediately threatened) apart from the ‘chill’ itself. . . . ‘Chilling effect’ is
17 cited as the *reason* why the governmental imposition is invalid rather than as the *harm*
18 which entitles the plaintiff to challenge it.” *United Presbyterian*, 738 F.2d at 1378
19 (citations omitted, emphasis original). In cases like this one that do not involve an
20 “exercise of governmental power [that is] regulatory, proscriptive, or compulsory in
21 nature,” *Laird*, 408 U.S. at 11, “mere subjective chilling effects,” such as those asserted by
22 the plaintiffs, “are simply not objectively discernable and are therefore not constitutionally
23 cognizable.” *Vernon v. City of Los Angeles*, 27 F.3d 1385, 1395 (9th Cir. 1994); *see also*
24 *Donohoe v. Duling*, 465 F.2d 196, 201-02 (4th Cir. 1972).

25 **2. Plaintiffs’ dissatisfaction with government policy does not give them standing.**

26 The FAC is, at its core, founded on disagreement with the government’s Terrorist
27 Surveillance Program. Plaintiffs’ interest in resolving this issue is no greater than that of
28 any other citizen who disagrees with the government’s conduct. In a democracy, this kind

1 of complaint is resolved by the political process, not the courts, especially not in a suit
2 against a private third-party. "Vindicating the *public* interest (including the public interest
3 in Government observance of the Constitution and laws) is the function of Congress and the
4 Chief Executive." *Lujan*, 504 U.S. at 576 (emphasis in original). Courts should address
5 such issues only as a last resort, and then only if an actual case or controversy is presented
6 by a plaintiff who incurs an injury that differs from that incurred by dissatisfied citizens in
7 general. *Valley Forge Christian College*, 454 U.S. at 473. "[A] plaintiff raising only a
8 generally available grievance about government – claiming only harm to his and every
9 citizen's interest in proper application of the Constitution and laws, and seeking relief that
10 no more directly and tangibly benefits him than it does the public at large – does not state
11 an Article III case or controversy." *Lujan*, 504 U.S. at 574-75.

12 Plaintiffs may sincerely believe that the Program is illegal and unconstitutional, but
13 that belief is not sufficient to create standing. Chief Justice Burger's observation in *Laird v.*
14 *Tatum* is particularly appropriate here:

15 Stripped to its essentials, what respondents appear to be seeking is a broad-
16 scale investigation, conducted by themselves as private parties armed with
17 the subpoena power of a federal district court and the power of cross-
18 examination, to probe into the Army's intelligence-gathering activities . . .
19 Carried to its logical end, this approach would have the federal courts as
20 virtually continuing monitors of the wisdom and soundness of Executive
21 action.

22 *Laird*, 408 U.S. at 14-15.

23 The Supreme Court has voiced these concerns on a number of occasions. *See also*,
24 *e.g.*, *Allen*, 468 U.S. at 750-61; *City of Los Angeles v. Lyons*, 461 U.S. 95, 111-12, 103 S.
25 Ct. 1660 (1983); *Schlesinger v. Reservists Committee to Stop the War*, 418 U.S. 208, 220-
26 23, 94 S. Ct. 2925 (1974); *O'Shea*, 414 U.S. 488, 492-95, 94 S. Ct. 669 (1974). Article III
27 courts are tribunals of limited jurisdiction, not vehicles for publicizing political conflicts or
28 roving commissions to enable more discovery or public disclosure of sensitive or classified
government programs than the Freedom of Information Act allows.

These concerns are at their apex when a plaintiff seeks to probe the executive's
conduct of foreign affairs. As this Court said in *In re World War II Era Japanese Forced*

1 *Labor Litig.*, 164 F. Supp. 2d 1160, 1170 (N.D. Cal. 2001), “[t]he Supreme Court has long
2 acknowledged the federal government’s broad authority over foreign affairs” and “observed
3 that the Constitution entrusts ‘the field of foreign affairs . . . to the President and the
4 Congress.’” (citations omitted).

5 For good reason, courts are loath to interfere with issues firmly within the province
6 of the legislative and executive branches of government. Public accounts of the Terrorist
7 Surveillance Program indicate that the executive branch uses it to gather foreign
8 intelligence and time-sensitive counterterrorism information and that it was approved by the
9 government’s most senior legal officials. Indeed, Congress is now reviewing this
10 understanding. *See, e.g.*, Terrorist Surveillance Act of 2006, S. 2455, 109th Cong., 2d Sess.
11 (introduced March 16, 2006). Few issues are less suited to judicial resolution than an
12 ongoing national policy dispute concerning the propriety of foreign intelligence activities.

13 **3. Plaintiffs fail to allege concrete injuries to their statutory interests.**

14 To have standing, a plaintiff must allege a concrete and personal stake in the
15 outcome of a lawsuit. The constitutional requirement of injury-in-fact is no less applicable
16 when violation of a statute is alleged. *O’Shea v. Littleton*, 414 U.S. at 493-94 (citing
17 *Baker v. Carr*, 369 U.S. 186, 204, 82 S. Ct. 691, 703 (1962); *United States v. SCRAP*,
18 412 U.S. 669, 687, 93 S. Ct. 2405, 2415 (1973)). “[S]tatutes do not purport to bestow the
19 right to sue in the absence of any indication that invasion of the statutory right has occurred
20 or is likely to occur.” *O’Shea*, 414 U.S. at 495 n.2.

21 Plaintiffs lack standing to assert their statutory claims (Counts II-VII) because the
22 FAC alleges no *facts* suggesting that their statutory rights have been violated. For example,
23 Count II asserts a claim under the criminal and civil liability provisions of the Foreign
24 Intelligence Surveillance Act (“FISA”), 50 U.S.C. §§ 1809, 1810. Plaintiffs allege “on
25 information and belief” that AT&T has installed or helped to install “interception devices
26 and pen registers and/or trap and trace devices” and conclude that AT&T has conducted
27 “electronic surveillance” (as defined in 50 U.S.C. § 1801). FAC ¶¶ 43, 93-94. But even if
28 true, these allegations are insufficient to establish that plaintiffs themselves suffered any

1 definite injury sufficient to entitle them to represent the class of individuals whose
2 communications they allege to have been intercepted. Plaintiffs' own allegations do not
3 make the facially absurd claim that *all* AT&T customers have been subjected to
4 surveillance by the government,¹³ and the FAC alleges nothing to suggest that the *named*
5 *plaintiffs* were themselves subject to surveillance. Because the named plaintiffs do not
6 allege facts demonstrating that, under the applicable FISA definitions, the government
7 actually acquired the content of their own communications,¹⁴ they are without standing.
8 The other counts of the FAC fare no better.¹⁵

9 **IV. CONCLUSION.**

10 For the foregoing reasons, the Amended Complaint should be dismissed.

11 Dated: April 28, 2006.

12 //

13 //

14 //

15

16

17

18 ¹³ For example, plaintiffs allege that interception devices "acquire the content of all *or a*
19 *substantial number of* the wire or electronic communications transferred through the
20 AT&T Corp. facilities *where they have been installed*" (emphasis added). FAC ¶ 44.
21 Similar allegations appear in ¶ 45 with respect to the use of pen registers and trap and
22 trace devices. Thus, plaintiffs appear to allege that some AT&T customers were not
23 subject to the surveillance alleged in the FAC: not all, but only a "substantial number" of
24 communications transferred by AT&T Corp. may have been subject to surveillance, and
25 only communications passing through certain facilities are even alleged to have been
26 subject to surveillance. Moreover, there is no allegation regarding whether or how the
27 government actually reviews or uses the data, if at all.

28 ¹⁴ Nor could they, as the facts necessary to support such an allegation would, even if they
existed, be classified and legally unavailable to any private party, including AT&T.

¹⁵ Counts III, IV, V and VI parrot the relevant statutory language, but no facts buttress the
legal conclusions that plaintiffs recite, and no actual injury is alleged. Plaintiffs'
allegation of unfair competition in violation of California Business and Professions Code
§ 17200 has the further standing flaw that plaintiffs failed to allege facts indicating that
they "suffered injury in fact and . . . lost money or property as a result of such unfair
competition." Cal. Bus. & Prof. Code §17204. Indeed, there is no suggestion that they
did not receive the telecommunications services for which they paid.

1 PILLSBURY WINTHROP
SHAW PITTMAN LLP
2 BRUCE A. ERICSON
DAVID L. ANDERSON
3 JACOB R. SORENSEN
MARC H. AXELBAUM
4 BRIAN J. WONG
50 Fremont Street
5 Post Office Box 7880
San Francisco, CA 94120-7880

SIDLEY AUSTIN LLP
DAVID W. CARPENTER
DAVID L. LAWSON
BRADFORD A. BERENSON
EDWARD R. MCNICHOLAS
1501 K Street, N.W.
Washington, D.C. 20005

6
7 By /s/ Bruce A. Ericson
Bruce A. Ericson

By /s/ Bradford A. Berenson
Bradford A. Berenson

8
9 Attorneys for Defendants AT&T CORP. and AT&T INC.
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

EXHIBIT D

1 PETER D. KEISLER
 Assistant Attorney General, Civil Division
 2 CARL J. NICHOLS
 Deputy Assistant Attorney General
 3 DOUGLAS N. LETTER
 Terrorism Litigation Counsel
 4 JOSEPH H. HUNT
 Director, Federal Programs Branch
 5 ANTHONY J. COPPOLINO
 Special Litigation Counsel
 6 tony.coppolino@usdoj.gov
 ANDREW H. TANNENBAUM
 7 andrew.tannenbaum@usdoj.gov
 Trial Attorney
 8 U.S. Department of Justice
 Civil Division, Federal Programs Branch
 9 20 Massachusetts Avenue, NW
 Washington, D.C. 20001
 10 Phone: (202) 514-4782/(202) 514-4263
 Fax: (202) 616-8460/(202) 616-8202/(202) 318-2461

11 Attorneys for Intervenor Defendant United States of America

12
 13 UNITED STATES DISTRICT COURT
 14 NORTHERN DISTRICT OF CALIFORNIA

15
 16 TASH HEPTING, GREGORY HICKS)
 CAROLYN JEWEL, and ERIK KNUTZEN)
 17 on Behalf of Themselves and All Others)
 Similarly Situated,)

18 Plaintiffs,)

19 v.)

20
 21 AT&T CORP., AT&T INC., and)
 22 DOES 1-20, inclusive,)

23 Defendants.)
 24

Case No. C 06-0672-VRW

NOTICE OF MOTION AND MOTION TO
 DISMISS OR, IN THE ALTERNATIVE,
 FOR SUMMARY JUDGMENT
 BY THE UNITED STATES OF AMERICA

Judge: The Hon. Vaughn R. Walker
 Hearing Date: June 21, 2006
 Courtroom: 6, 17th Floor

25
 26
 27 NOTICE OF MOTION AND MOTION TO DISMISS, OR, IN THE ALTERNATIVE, FOR SUMMARY
 JUDGMENT BY THE UNITED STATES OF AMERICA
 28 Case No. C 06-0672-VRW

1 PLEASE TAKE NOTICE that, on June 21, 2006,¹ before the Honorable Vaughn R.
2 Walker, intervenor United States of America will move for an order dismissing this action,
3 pursuant to Rules 12(b)(1) and 12(b)(6) of the Federal Rules of Civil Procedure, or, in the
4 alternative, for summary judgment, pursuant to Rule 56 of the Federal Rules of Civil Procedure.
5 As explained in the United States' unclassified memorandum as well as the memorandum
6 submitted *ex parte* and *in camera*, the United States' invocation of the military and state secrets
7 privilege and of specified statutory privileges requires dismissal of this action, or, in the
8 alternative, summary judgment in favor of the United States.

9 Respectfully submitted,

10 PETER D. KEISLER
11 Assistant Attorney General, Civil Division

12 CARL J. NICHOLS
13 Deputy Assistant Attorney General

14 DOUGLAS N. LETTER
15 Terrorism Litigation Counsel

16 JOSEPH H. HUNT
17 Director, Federal Programs Branch

18 *s/Anthony J. Coppolino*
19 ANTHONY J. COPPOLINO
20 Special Litigation Counsel
21 tony.coppolino@usdoj.gov

22 *s/Andrew H. Tannenbaum*
23 ANDREW H. TANNENBAUM
24 Trial Attorney
25 andrew.tannenbaum@usdoj.gov
26 U.S. Department of Justice
27 Civil Division, Federal Programs Branch
28 20 Massachusetts Avenue, NW
Washington, D.C. 20001

24 ¹ The United States has filed an Administrative Motion to Set Hearing Date for the United
25 States' Motions requesting that the Court set the hearing date for this motion and the United
26 States' Motion To Intervene, for June 21, 2006 – the present hearing date for Plaintiffs' Motion
for Preliminary Injunction.

27 NOTICE OF MOTION AND MOTION TO DISMISS, OR, IN THE ALTERNATIVE, FOR SUMMARY
28 JUDGMENT BY THE UNITED STATES OF AMERICA

Case No. C 06-0672-VRW

Phone: (202) 514-4782/(202) 514-4263
Fax: (202) 616-8460/(202) 616-8202/(202) 318-2461

Attorneys for Intervenor Defendant United States

DATED: May 12, 2006

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11
- 12
- 13
- 14
- 15
- 16
- 17
- 18
- 19
- 20
- 21
- 22
- 23
- 24
- 25
- 26
- 27
- 28

1 PETER D. KEISLER
 2 Assistant Attorney General
 CARL J. NICHOLS
 3 Deputy Assistant Attorney General
 DOUGLAS N. LETTER
 4 Terrorism Litigation Counsel
 JOSEPH H. HUNT
 5 Director, Federal Programs Branch
 ANTHONY J. COPPOLINO
 6 Special Litigation Counsel
tony.coppolino@usdoj.gov
 7 ANDREW H. TANNENBAUM
andrew.tannenbaum@usdoj.gov
 8 Trial Attorney
 9 U.S. Department of Justice
 10 Civil Division, Federal Programs Branch
 11 20 Massachusetts Avenue, NW
 Washington, D.C. 20001
 12 Phone: (202) 514-4782/(202) 514-4263
 13 Fax: (202) 616-8460/(202) 616-8202
Attorneys for the United States of America

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

17 TASH HEPTING, GREGORY HICKS,)
 18 CAROLYN JEWEL, and ERIK KNUTZEN,)
 On Behalf of Themselves and All Others)
 19 Similarly Situated,)
 20 Plaintiffs,)
 21 v.)
 22 AT&T CORP., AT&T INC., and)
 23 DOES 1-20, inclusive,)
 24 Defendants.)
 25

Case No. C-06-0672-VRW

**MEMORANDUM OF THE
UNITED STATES IN SUPPORT
OF THE MILITARY AND
STATE SECRETS PRIVILEGE
AND MOTION TO DISMISS OR,
IN THE ALTERNATIVE, FOR
SUMMARY JUDGMENT**

Hon. Vaughn R. Walker

(U) INTRODUCTION

1
2 (U) The United States of America, through its undersigned counsel, hereby submits this
3 Memorandum of Points and Authorities in support of the assertion of the military and state
4 secrets privilege (commonly known as the "state secrets privilege")¹ by the Director of National
5 Intelligence ("DNI"), and related statutory privilege assertions by the DNI and the Director of
6 the National Security Agency ("DIRNSA").² Through these assertions of privilege, the United
7 States seeks to protect certain intelligence activities, information, sources, and methods,
8 implicated by the allegations in this case. The information to be protected is described herein, in
9 a separate memorandum lodged for the Court's *in camera*, *ex parte* consideration, and in public
10 and classified declarations submitted by the DNI and DIRNSA.³ For the reasons set forth in
11 those submissions, the disclosure of the information to which these privilege assertions apply
12 would cause exceptionally grave harm to the national security of the United States.

13
14 (U) In addition, the United States has also moved to intervene in this action, pursuant to
15 Rule 24 of the Federal Rules of Civil Procedure, for the purpose of seeking dismissal of this
16 action or, in the alternative, summary judgment. As set forth below, this case cannot be litigated
17 because adjudication of Plaintiffs' claims would put at risk the disclosure of privileged national
18 security information.
19
20
21

22 ¹ (U) The phrase "state secrets privilege" is often used in this memorandum to refer
23 collectively to the military and state secrets privilege and the statutory privileges invoked in this
24 case.

25 ² (U) This submission is made pursuant to 28 U.S.C. § 517, as well as pursuant to the
26 Federal Rules of Civil Procedure.

27 ³ (U) The classified declarations of John D. Negroponte, DNI, and Keith B. Alexander,
28 DIRNSA, as well as the separately lodged memorandum for the Court's *in camera*, *ex parte*
consideration, are currently stored in a proper secure location by the Department of Justice and
are available for review by the Court upon request.

1 [REDACTED TEXT]

2 (U) The state secrets privilege has long been recognized for protecting information vital
3 to the nation's security or diplomatic relations. See *United States v. Reynolds*, 345 U.S. 1
4 (1953); *Kasza v. Browner*, 133 F.3d 1159 (9th Cir.), cert. denied, 525 U.S. 967 (1998). "Once
5 the privilege is properly invoked and the court is satisfied that there is a reasonable danger that
6 national security would be harmed by the disclosure of state secrets, the privilege is absolute,"
7 and the information at issue must be excluded from disclosure and use in the case. *Kasza*, 133
8 F.3d at 1166. Moreover, if "the 'very subject matter of the action' is a state secret, then the court
9 should dismiss the plaintiff's action based solely on the invocation of the state secrets privilege."
10 *Kasza*, 133 F.3d at 1166. In such cases, "sensitive military secrets will be so central to the
11 subject matter of the litigation that any attempt to proceed will threaten disclosure of the
12 privileged matters." See *Fitzgerald v. Penthouse Int'l, Ltd.*, 776 F.2d 1236 (4th Cir. 1985).
13 Dismissal is also necessary when either the plaintiff cannot make out a prima facie case in
14 support of its claims absent the excluded state secrets, or if the privilege deprives the defendant
15 of information that would otherwise provide a valid defense to the claim. *Kasza*, 133 F.3d at
16 1166.
17
18
19

20 [REDACTED TEXT]

21 (U) BACKGROUND

22 A. (U) September 11, 2001

23 (U) On September 11, 2001, the al Qaeda terrorist network launched a set of coordinated
24 attacks along the East Coast of the United States. Four commercial jetliners, each carefully
25 selected to be fully loaded with fuel for a transcontinental flight, were hijacked by al Qaeda
26 operatives. Those operatives targeted the Nation's financial center in New York with two of the
27
28

1 jetliners, which they deliberately flew into the Twin Towers of the World Trade Center. Al
2 Qaeda targeted the headquarters of the Nation's Armed Forces, the Pentagon, with the third
3 jetliner. Al Qaeda operatives were apparently headed toward Washington, D.C. with the fourth
4 jetliner when passengers struggled with the hijackers and the plane crashed in Shanksville,
5 Pennsylvania. The intended target of this fourth jetliner was most evidently the White House or
6 the Capitol, strongly suggesting that al Qaeda's intended mission was to strike a decapitation
7 blow to the Government of the United States—to kill the President, the Vice President, or
8 Members of Congress. The attacks of September 11 resulted in approximately 3,000 deaths—
9 the highest single-day death toll from hostile foreign attacks in the Nation's history. In addition,
10 these attacks shut down air travel in the United States, disrupted the Nation's financial markets
11 and Government operations, and caused billions of dollars of damage to the economy.
12
13

14 (U) On September 14, 2001, the President declared a national emergency "by reason of
15 the terrorist attacks at the World Trade Center, New York, New York, and the Pentagon, and the
16 continuing and immediate threat of further attacks on the United States." Proclamation No.
17 7463, 66 Fed. Reg. 48199 (Sept. 14, 2001). The United States also launched a massive military
18 response, both at home and abroad. In the United States, combat air patrols were immediately
19 established over major metropolitan areas and were maintained 24 hours a day until April 2002.
20 The United States also immediately began plans for a military response directed at al Qaeda's
21 training grounds and haven in Afghanistan. On September 14, 2001, both Houses of Congress
22 passed a Joint Resolution authorizing the President "to use all necessary and appropriate force
23 against those nations, organizations, or persons he determines planned, authorized, committed, or
24 aided the terrorist attacks" of September 11. Authorization for Use of Military Force, Pub. L.
25 No. 107-40 § 21(a), 115 Stat. 224, 224 (Sept. 18, 2001) ("Cong. Auth."). Congress also
26
27
28

1 expressly acknowledged that the attacks rendered it "necessary and appropriate" for the United
2 States to exercise its right "to protect United States citizens both at home and abroad," and
3 acknowledged in particular that the "the President has authority under the Constitution to take
4 action to deter and prevent acts of international terrorism against the United States." *Id.* pmb1.

5
6 (U) As the President made clear at the time, the attacks of September 11 "created a state
7 of armed conflict." Military Order, § 1(a), 66 Fed. Reg. 57833, 57833 (Nov. 13, 2001). Indeed,
8 shortly after the attacks, NATO took the unprecedented step of invoking article 5 of the North
9 Atlantic Treaty, which provides that an "armed attack against one or more of [the parties] shall
10 be considered an attack against them all." North Atlantic Treaty, Apr. 4, 1949, art. 5, 63 Stat.
11 2241, 2244, 34 U.N.T.S. 243, 246; see also Statement by NATO Secretary General Lord
12 Robertson (Oct. 2, 2001), available at <http://www.nato.int/docu/speech/2001/s011002a.htm> ("[I]t
13 has now been determined that the attack against the United States on 11 September was directed
14 from abroad and shall therefore be regarded as an action covered by Article 5 of the Washington
15 Treaty . . ."). The President also determined that al Qaeda terrorists "possess both the capability
16 and the intention to undertake further terrorist attacks against the United States that, if not
17 detected and prevented, will cause mass deaths, mass injuries, and massive destruction of
18 property, and may place at risk the continuity of the operations of the United States
19 Government," and he concluded that "an extraordinary emergency exists for national defense
20 purposes." Military Order, § 1(c), (g), 66 Fed. Reg. at 57833-34.

21
22
23
24 **B. (U) The Continuing Terrorist Threat Posed by al Qaeda**

25 (U) With the attacks of September 11, Al Qaeda demonstrated its ability to introduce
26 agents into the United States undetected and to perpetrate devastating attacks. But, as the
27 President has made clear, "[t]he terrorists want to strike America again, and they hope to inflict
28

1 even more damage than they did on September the 11th.” Press Conference of President Bush
2 (Dec. 19, 2005).⁴ For this reason, as the President explained, finding al Qaeda sleeper agents in
3 the United States remains one of the paramount national security concerns to this day. *See id.*

4 (U) Since the September 11 attacks, al Qaeda leaders have repeatedly promised to
5 deliver another, even more devastating attack on America. For example, in October 2002, al
6 Qaeda leader Ayman al-Zawahiri stated in a video addressing the “citizens of the United States”:
7 “I promise you that the Islamic youth are preparing for you what will fill your hearts with
8 horror.” In October 2003, Osama bin Laden stated in a released videotape that “We, God
9 willing, will continue to fight you and will continue martyrdom operations inside and outside the
10 United States” And again in a videotape released on October 24, 2004, bin Laden warned
11 U.S. citizens of further attacks and asserted that “your security is in your own hands.” In recent
12 months, al Qaeda has reiterated its intent to inflict a catastrophic terrorist attack on the United
13 States. On December 7, 2005, al-Zawahiri professed that al Qaeda “is spreading, growing, and
14 becoming stronger,” and that al Qaeda is “waging a great historic battle in Iraq, Afghanistan,
15 Palestine, and even in the Crusaders’ own homes.” Finally, as is well known, since September
16 11, al Qaeda has staged several large-scale attacks around the world, including in Indonesia,
17 Madrid, and London, killing hundreds of innocent people.
18
19
20

21 [REDACTED TEXT]

22 C. (U) Intelligence Challenges After September 11, 2001

23 [REDACTED TEXT]
24
25
26
27

28 ⁴ (U) Available at <http://www.white-house.gov/news/releases/2005/12/20051219-2.html>.

1 D. (U) NSA Activities Critical to Meeting Post-9/11 Intelligence Challenges

2 [REDACTED TEXT]

3 E. (U) Plaintiffs' Claims

4 (U) Against this backdrop, upon the media disclosures in December 2005 of certain post-
5 9/11 intelligence gathering activities, Plaintiffs filed this suit alleging that the Government is
6 conducting a massive surveillance program, vacuuming up and searching the content of
7 communications engaged in by millions of AT&T customers. While clearly putting purported
8 Government activities at issue, *see* Am. Compl. ¶ 3, Plaintiffs filed suit against AT&T, alleging
9 that it illegally provides the NSA with direct access to key facilities and databases and discloses
10 to the Government the content of telephone and electronic communications as well as detailed
11 communications records about millions of customers. *See* Am. Complaint ¶¶ 3-6.

12
13
14 (U) Plaintiffs first put at issue NSA's activities in connection with the TSP, which was
15 publicly described by the President in December 2005, alleging that "NSA began a classified
16 surveillance program shortly after September 11, 2001 to intercept the communications within
17 the United States without judicial warrant." *See* Am. Compl. ¶ 32-37. Plaintiffs also allege that
18 as part of this "data mining" program, "the NSA intercepts millions of communications made or
19 received by people inside the United States, and uses powerful computers to scan their contents
20 for particular names, numbers, words, or phrases." *Id.* ¶ 39. Plaintiffs allege in particular that
21 AT&T has assisted the Government in installing "interception devices," "pen registers" and "trap
22 and trace" devices in order to "acquire the content" of communications and receive "dialing,
23 routing, addressing, or signaling information." *Id.* ¶¶ 42-47.

24
25
26 (U) Plaintiffs seek declaratory and injunctive relief and damages under various federal
27 and state statutory provisions and the First and Fourth Amendments, Am. Compl. ¶¶ 65-66 &
28

1 Counts II-VI, and also seek declaratory and injunctive relief under the First and Fourth
2 Amendments on the theory that the Government has instigated, directed, or tacitly approved the
3 alleged actions by AT&T, and that AT&T acts as an instrument or agent of the Government. *Id.*
4 ¶¶ 66, 82, 85 & Count I. Finally, Plaintiffs have also moved for a preliminary injunction that
5 would, *inter alia*, enjoin AT&T “from facilitating the interception, use, or disclosure of its
6 customers’ communications by or to the United States Government,” except pursuant to a court
7 order or an emergency authorization of the Attorney General. *See* [Proposed] Order Granting
8 Preliminary Injunction (Docket No. 17) ¶ 3.

10 **(U) ARGUMENT**

11 [REDACTED TEXT]

13 **I. (U) THE STATE SECRETS PRIVILEGE BARS USE OF PRIVILEGED INFORMATION REGARDLESS OF A LITIGANT’S NEED.**

14 (U) The ability of the executive to protect military or state secrets from disclosure has
15 been recognized from the earliest days of the Republic. *See Totten v. United States*, 92 U.S. 105
16 (1875); *United States v. Burr*, 25 F. Cas. 30 (C.C.D. Va. 1807); *Reynolds*, 345 U.S. at 6-7. The
17 privilege derives from the President’s Article II powers to conduct foreign affairs and provide for
18 the national defense. *United States v. Nixon*, 418 U.S. 683, 710 (1974). Accordingly, it “must
19 head the list” of evidentiary privileges. *Halkin I*, 598 F.2d at 7.

22 **A. (U) Procedural Requirements**

23 (U) As a procedural matter, “[t]he privilege belongs to the Government and must be
24 asserted by it; it can neither be claimed nor waived by a private party.” *Reynolds*, 345 U.S. at 7;
25 *see also Kasza*, 133 F.3d at 1165. “There must be a formal claim of privilege, lodged by the
26 head of the department which has control over the matter, after actual personal consideration by
27 the officer.” *Reynolds*, 345 U.S. at 7-8 (footnotes omitted). Thus, the responsible agency head

28 MEMORANDUM OF THE UNITED STATES IN SUPPORT
OF STATE SECRETS PRIVILEGE AND MOTION TO DISMISS
OR, IN THE ALTERNATIVE, FOR SUMMARY JUDGMENT
CASE NO. C-06-0672-VRW

1 must personally consider the matter and formally assert the claim of privilege.

2 **B. (U) Information Covered**

3 (U) The privilege protects a broad range of state secrets, including information that would
4 result in "impairment of the nation's defense capabilities, disclosure of intelligence-gathering
5 methods or capabilities, and disruption of diplomatic relations with foreign Governments."

6 *Ellsberg v. Mitchell*, 709 F.2d 51, 57 (D.C. Cir. 1983), *cert. denied sub nom. Russo v. Mitchell*,
7 465 U.S. 1038 (1984) (footnotes omitted); *accord Kasza*, 133 F.3d at 1166 ("[T]he Government
8 may use the state secrets privilege to withhold a broad range of information;"); *see also Halkin v.*
9 *Helms (Halkin II)*, 690 F.2d 977, 990 (D.C. Cir. 1982) (state secrets privilege protects
10 intelligence sources and methods involved in NSA surveillance). In addition, the privilege
11 extends to protect information that, on its face, may appear innocuous but which in a larger
12 context could reveal sensitive classified information: *Kasza*, 133 F.3d at 1166.

13
14
15 It requires little reflection to understand that the business of foreign intelligence
16 gathering in this age of computer technology is more akin to the construction of a
17 mosaic than it is to the management of a cloak and dagger affair. Thousands of
18 bits and pieces of seemingly innocuous information can be analyzed and fitted
19 into place to reveal with startling clarity how the unseen whole must operate.

20 *Halkin I*, 598 F.2d at 8. "Accordingly, if seemingly innocuous information is part of a classified
21 mosaic, the state secrets privilege may be invoked to bar its disclosure and the court cannot order
22 the Government to disentangle this information from other classified information." *Kasza*, 133
23 F.3d at 1166.

24 **C. (U) Standard of Review**

25 (U) An assertion of the state secrets privilege "must be accorded the 'utmost deference'
26 and the court's review of the claim of privilege is narrow." *Kasza*, 133 F.3d at 1166. Aside
27 from ensuring that the privilege has been properly invoked as a procedural matter, the sole
28

1 determination for the court is whether, “under the particular circumstances of the case, ‘there is a
2 reasonable danger that compulsion of the evidence will expose military matters which, in the
3 interest of national security, should not be divulged.’” *Kasza*, 133 F.3d at 1166 (quoting
4 *Reynolds*, 345 U.S. at 10); *see also In re United States*, 872 F.2d 472, 475-76 (D.C. Cir. 1989);
5 *Tilden v. Tenet*, 140 F. Supp. 2d 623, 626 (E.D. Va. 2000).

6
7 (U) Thus, in assessing whether to uphold a claim of privilege, the court does not balance
8 the respective needs of the parties for the information. Rather, “[o]nce the privilege is properly
9 invoked and the court is satisfied that there is a reasonable danger that national security would be
10 harmed by the disclosure of state secrets, the privilege is absolute[.]” *Kasza*, 133 F.3d at 1166;
11 *see also In re Under Seal*, 945 F.2d at 1287 n.2 (state secrets privilege “renders the information
12 unavailable regardless of the other party’s need in furtherance of the action”); *Northrop Corp. v.*
13 *McDonnell Douglas Corp.*, 751 F.2d 395, 399 (D.C. Cir. 1984) (state secrets privilege “cannot
14 be compromised by any showing of need on the part of the party seeking the information”);
15 *Ellsberg*, 709 F.2d at 57 (“When properly invoked, the state secrets privilege is absolute. No
16 competing public or private interest can be advanced to compel disclosure of information found
17 to be protected by a claim of privilege.”). The court may consider the necessity of the
18 information to the case only in connection with assessing the sufficiency of the Government’s
19 showing that there is a reasonable danger that disclosure of the information at issue would harm
20 national security. “[T]he more plausible and substantial the Government’s allegations of danger
21 to national security, in the context of all the circumstances surrounding the case, the more
22 deferential should be the judge’s inquiry into the foundations and scope of the claim.” *Id.* at 59.

23
24
25
26 Where there is a strong showing of necessity, the claim of privilege should not be
27 lightly accepted, but even the most compelling necessity cannot overcome the
28 claim of privilege if the court is ultimately satisfied that military secrets are at
stake.

1 *Reynolds*, 345 U.S. at 11; *Kasza*, 133 F.3d at 1166.

2 (U) Judicial review of whether the claim of privilege has been properly asserted and
3 supported does not require the submission of classified information to the court for *in camera*, *ex*
4 *parte* review. In particular, where it is possible to satisfy the court, from all the circumstances of
5 the case, that there is a reasonable danger that compulsion of the evidence will expose state
6 secrets which, in the interest of national security, should not be divulged, "the occasion for the
7 privilege is appropriate, and the court should not jeopardize the security which the privilege is
8 meant to protect by insisting upon an examination of the evidence, even by the judge alone, in
9 chambers." *Reynolds*, 345 U.S. at 8. Indeed, one court has observed that *in camera*, *ex parte*
10 review itself may not be "entirely safe."
11

12 It is not to slight judges, lawyers or anyone else to suggest that any such
13 disclosure carries with it serious risk that highly sensitive information may be
14 compromised. In our own chambers, we are ill equipped to provide the kind of
15 security highly sensitive information should have.

16 *Clift v. United States*, 597 F.2d 826, 829 (2d Cir. 1979) (quoting *Alfred A. Knopf, Inc. v. Colby*,
17 509 F.2d 1362, 1369 (4th Cir.), *cert. denied*, 421 U.S. 992 (1975)).
18

19 (U) Nonetheless, the submission of classified declarations for *in camera*, *ex parte* review
20 is "unexceptional" in cases where the state secrets privilege is invoked. *Kasza*, 133 F.3d at 1169
21 (citing *Black v. United States*, 62 F.3d 1115 (8th Cir. 1995), *cert. denied*, 517 U.S. 1154 (1996));
22 *see Zuckerbraun v. General Dynamics Corp.*, 935 F.2d 544 (2d Cir. 1991); *Fitzgerald v.*
23 *Penthouse Int'l, Ltd.*, 776 F.2d 1236 (4th Cir. 1985); *Molerio v. FBI*, 749 F.2d 815, 819, 822
24 (D.C. Cir. 1984); *Farnsworth Cannon, Inc. v. Grimes*, 635 F.2d 268, 281 (4th Cir. 1980) (en
25 banc); *see also, e.g., In re United States*, 872 F.2d at 474 (classified declaration of assistant
26 director of the FBI's Intelligence Division submitted for *in camera* review in support of Attorney
27

1 General's formal invocation of state secrets privilege).

2 **II. (U) THE UNITED STATES PROPERLY HAS ASSERTED THE STATE**
3 **SECRETS PRIVILEGE AND ITS CLAIM OF PRIVILEGE SHOULD BE**
4 **UPHELD.**

5 **A. (U) The United States Properly Has Asserted the State Secrets**
6 **Privilege.**

7 (U) It cannot be disputed that the United States properly has asserted the state secrets
8 privilege in this case. The Director of National Intelligence, who bears statutory authority as
9 head of the United States Intelligence Community to protect intelligence sources and methods,
10 see 50 U.S.C. § 403-1(i)(1), has formally asserted the state secrets privilege after personal
11 consideration of the matter. See *Reynolds*, 345 U.S. at 7-8.⁵ DNI Negroponte has submitted an
12 unclassified declaration and an *in camera, ex parte* classified declaration, both of which state that
13 the disclosure of the intelligence information, sources, and methods described herein would
14 cause exceptionally grave harm to the national security of the United States. See *Public and In*
15 *Camera, Ex Parte* Declarations of John D. Negroponte, Director of National Intelligence. Based
16 on this assertion of privilege by the head of the United States intelligence community, the
17 Government's claim of privilege has been properly lodged.

19 **B. (U) The United States Has Demonstrated that There is a Reasonable Danger**
20 **that Disclosure of the Intelligence Information, Sources, and Methods**
21 **Implicated by Plaintiffs' Claims Would Harm the National Security of the**
22 **United States.**

23 (U) The United States also has demonstrated that there is a reasonable danger that
24 disclosure of the information subject to the state secrets privilege would harm U.S. national
25 security. *Kasza*, 133 F.3d at 1170. While "the Government need not demonstrate that injury to
26

27
28 ⁵ (U) See 50 U.S.C. § 401a(4) (including the National Security Agency is included in the
United States "Intelligence Community").

1 the national interest will inevitably result from disclosure," *Ellsberg, supra*, 709 F.2d at 58, the
2 showing made here is more than reasonable, and highly compelling.

3 (U) DNI Negroponte, supported by the *Ex Parte, In Camera* Declaration of General
4 Alexander, has asserted the state secrets privilege and demonstrated the exceptional harm that
5 would be caused to U.S. national security interests by disclosure of each of the following the
6 categories of privileged information at issue in this case.
7

8 [REDACTED TEXT]

9 (U) Each of the foregoing categories of information is subject to DNI Negroponte's state
10 secrets privilege claim, and he and General Alexander have amply demonstrated a reasoned basis
11 that disclosure of this information would cause exceptionally grave damage to the national
12 security and, therefore, that this information should be excluded from this case.
13

14 **C. (U) Statutory Privilege Claims Have Also Been Properly Raised in This Case.**

15 (U) Two statutory protections also apply to the intelligence-related information, sources
16 and methods described herein, and both have been properly invoked here as well. First, Section
17 6 of the National Security Agency Act of 1959, Pub. L. No. 86-36, § 6, 73 Stat. 63, 64, codified
18 at 50 U.S.C. § 402 note, provides:
19

20 [N]othing in this Act or any other law . . . shall be construed to require the
21 disclosure of the organization or any function of the National Security Agency,
22 of any information with respect to the activities thereof, or of the names, titles,
23 salaries, or number of persons employed by such agency.

24 *Id.* Section 6 reflects a "congressional judgment that in order to preserve national security,
25 information elucidating the subjects specified ought to be safe from forced exposure." *The*
26 *Founding Church of Scientology of Washington, D.C., Inc. v. Nat'l Security Agency*, 610 F.2d
27 824, 828 (D.C. Cir. 1979); *accord Hayden v. Nat'l Security Agency*, 608 F.2d 1381, 1389 (D.C.
28 Cir. 1979). In enacting Section 6, Congress was "fully aware of the 'unique and sensitive'

1 activities of the [NSA] which require 'extreme security measures.'" *Hayden*, 608 F.2d at 1390
2 (citing legislative history). Thus, "[t]he protection afforded by section 6 is, by its very terms,
3 absolute. If a document is covered by section 6, NSA is entitled to withhold it. . . ." *Linder v.*
4 *Nat'l Security Agency*, 94 F.3d 693, 698 (D.C. Cir. 1996).

5 (U) The second applicable statute is Section 102A(i)(1) of the Intelligence Reform and
6 Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638 (Dec. 17, 2004), codified
7 at 50 U.S.C. § 403-1(i)(1). This statute requires the Director of National Intelligence to "protect
8 intelligence sources and methods from unauthorized disclosure. The authority to protect
9 intelligence sources and methods from disclosure is rooted in the "practical necessities of
10 modern intelligence gathering," *Fitzgibbon v. CIA*, 911 F.2d 755, 761 (D.C. Cir. 1990), and has
11 been described by the Supreme Court as both "sweeping," *CIA v. Sims*, 471 U.S. 159, 169
12 (1985), and "wideranging." *Snepp v. United States*, 444 U.S. 507, 509 (1980). Sources and
13 methods constitute "the heart of all intelligence operations," *Sims*, 471 U.S. at 167, and "[i]t is
14 the responsibility of the [intelligence community], not that of the judiciary to weigh the variety
15 of complex and subtle factors in determining whether disclosure of information may lead to an
16 unacceptable risk of compromising the . . . intelligence-gathering process." *Id.* at 180.

17 (U) These statutory privileges have been properly asserted as to any intelligence-related
18 information, sources and methods implicated by Plaintiffs' claims and the information covered
19 by these privilege claims are at least co-extensive with the assertion of the state secrets privilege
20 by the DNI. *See* Public Declaration of John D. Negroponte, Director of National Intelligence,
21 and Public Declaration of Keith T. Alexander, Director of the National Security Agency.

22 **III. (U) THE STATE SECRETS PRIVILEGE REQUIRES DISMISSAL OF THIS**
23 **ACTION.**

24 (U) Once the court has upheld a claim of the state secrets privilege, the evidence and
25

1 information identified in the privilege assertion is removed from the case, and the Court must
2 undertake a separate inquiry to determine the consequences of this exclusion on further
3 proceedings.

4 (U) If “the ‘very subject matter of the action’ is a state secret, then the court should
5 dismiss the plaintiff’s action based solely on the invocation of the state secrets privilege.” *Kasza*,
6 133 F.3d at 1166 (citing *Reynolds*, 345 U.S. at 11 n. 26); *see also Totten v. United States*, 92 U.S.
7 (2 Otto) 105, 107, 23 L.Ed. 605 (1875) (“[P]ublic policy forbids the maintenance of any suit in a
8 court of justice, the trial of which would inevitably lead to the disclosure of matters which the
9 law itself regards as confidential, and respecting which it will not allow the confidence to be
10 violated.”); *Weston v. Lockheed Missiles & Space Co.*, 881 F.2d 814, 816 (9th Cir. 1989)
11 (recognizing that state secrets privilege alone can be the basis of dismissal of a suit). In such
12 cases, “sensitive military secrets will be so central to the subject matter of the litigation that any
13 attempt to proceed will threaten disclosure of the privileged matters.” *Fitzgerald*, 776 F.2d at
14 1241-42. *See also Maxwell v. First National Bank of Maryland*, 143 F.R.D. 590, 598-99 (D. Md.
15 1992); *Edmonds v. U.S. Department of Justice*, 323 F. Supp. 2d 65, 77-82 (D.D.C. 2004), *aff’d*,
16 161 Fed. Appx. 6, 045286 (D.C. Cir. May 6, 2005) (*per curiam* judgment), *cert. denied*, 126 S.
17 Ct. 734 (2005); *Tilden*, 140 F. Supp. 2d at 626.

18 (U) Even if the very subject matter of an action is not a state secret, if the plaintiff cannot
19 make out a prima facie case in support of its claims absent the excluded state secrets, the case
20 must be dismissed. *See Kasza*, 133 F.3d at 1166; *Halkin II*, 690 F.2d at 998-99; *Fitzgerald*, 776
21 F.2d at 1240-41. And if the privilege “deprives the *defendant* of information that would
22 otherwise give the defendant a valid defense to the claim, then the court may grant summary
23 judgment to the defendant.” *Kasza*, 133 F.3d at 1166 (quoting *Bareford v. General Dynamics*
24
25
26
27
28

1 *Corp.*, 973 F.2d 1138, 1141 (5th Cir. 1992)); *see also Molerio v. FBI*, 749 F.2d 815, 825 (D.C.
2 Cir. 1984) (granting summary judgment where state secrets privilege precluded the Government
3 from using a valid defense).

4 [REDACTED TEXT]

5 A. (U) Further Litigation Would Inevitably Risk the Disclosure of State Secrets.

6 [REDACTED TEXT]

7 B. (U) Information Subject to the State Secrets Privilege is
8 Necessary to Adjudicate Plaintiffs' Claims.

9
10 (U) Beyond the foregoing concerns, it should also be apparent that any attempt to litigate
11 the merits of the Plaintiffs' claims will require the disclosure of information covered by the state
12 secrets assertion. Adjudicating each claim in the Amended Complaint would require
13 confirmation or denial of the existence, scope, and potential targets of alleged intelligence
14 activities, as well as AT&T's alleged involvement in such activities. Because such information
15 cannot be confirmed or denied without causing exceptionally grave damage to the national
16 security, every step in this case—either for Plaintiffs to prove their claims, for Defendants to
17 defend them, or for the United States to represent its interests—runs into privileged information.
18

19
20 1. (U) Plaintiffs Cannot Establish Standing

21 (U) As a result of the Government's state secrets assertion, Plaintiffs will not be able to
22 prove that they have standing to litigate their claims. Plaintiffs, of course, bear the burden of
23 establishing standing and must, at an "irreducible constitutional minimum," demonstrate (1) an
24 injury-in-fact, (2) a causal connection between the injury and the conduct complained of, and (3)
25 a likelihood that the injury will be redressed by a favorable decision. *Lujan v. Defenders of*
26 *Wildlife*, 504 U.S. 555, 560-61 (1992). In meeting that burden, the named Plaintiffs must
27
28

1 demonstrate an actual or imminent—not speculative or hypothetical—injury that is particularized
2 as to them; they cannot rely on alleged injuries to unnamed members of a purported class.⁶
3 Moreover, to obtain prospective relief, Plaintiffs must show that they are “immediately in danger
4 of sustaining some direct injury” as the result of the challenged conduct. *City of Los Angeles v.*
5 *Lyons*, 461 U.S. 95, 102 (1983); *O’Shea v. Littleton*, 414 U.S. 488, 495-96 (1974).⁷ In addition
6 to the constitutional requirements of Article III, Plaintiffs must also satisfy prudential standing
7 requirements, including that they “assert [their] own legal interests rather than those of third
8 parties,” *Phillips Petroleum Co. v. Shutts*, 472 U.S. 797, 804 (1985), and that their claim not be a
9 “generalized grievance” shared in substantially equal measure by all or a large class of citizens.
10 *Warth v. Seldin*, 422 U.S. 499 (1975).
11

12
13 (U) Plaintiffs cannot prove these elements without information covered by the state
14 secrets assertion.⁸ The Government’s privilege assertion covers any information tending to
15

16
17 ⁶ (U) *See, e.g., Warth v. Seldin*, 422 U.S. 490, 502 (1975) (the named plaintiffs in an
18 action “must allege and show that they personally have been injured, not that injury has been
19 suffered by other, unidentified members of the class to which they belong and which they
20 purport to represent”).

21 ⁷ (U) Standing requirements demand the “strictest adherence” when, like here,
22 constitutional questions are presented and “matters of great national significance are at stake.”
23 *Elk Grove Unified Sch. Dist. v. Newdow*, 542 U.S. 1, 11 (2004); *see also Raines v. Byrd*, 521
24 U.S. 811, 819-20 (1997) (“[O]ur standing inquiry has been especially rigorous when reaching the
25 merits of the dispute would force us to decide whether an action taken by one of the other two
26 branches of the Federal Government was unconstitutional.”); *Schlesinger v. Reservists Comm. to*
27 *Stop the War*, 418 U.S. 208, 221 (1974) (“[W]hen a court is asked to undertake constitutional
28 adjudication, the most important and delicate of its responsibilities, the requirement of concrete
injury further serves the function of insuring that such adjudication does not take place
unnecessarily.”).

29 ⁸ (U) The focus herein is on Plaintiffs’ inability to prove standing because it is their
30 burden to demonstrate jurisdiction. *See Lujan*, 504 U.S. at 561. Dismissal of this action,
31 however, is also required for the equally important reason that AT&T and the Government
32 would not be able to present any evidence disproving standing on any claim without revealing
33 information covered by the state secrets privilege assertion (e.g., whether or not a particular
34 person’s communications were intercepted). *See Halkin I*, 598 F.2d at 11 (rejecting plaintiffs’

1 confirm or deny (a) the alleged intelligence activities, (b) whether AT&T was involved with any
2 such activity, and (c) whether a particular individual's communications were intercepted as a
3 result of any such activity. See Public Declaration of John D. Negroponte. Without these
4 facts—which should be removed from the case as a result of the state secrets assertion—
5 Plaintiffs cannot establish any alleged injury that is fairly traceable to AT&T. Thus, regardless
6 of whether they adequately allege such facts, Plaintiffs ultimately will not be able to prove
7 injury-in-fact or causation.⁹

9 (U) In such circumstances, courts have held that the assertion of the state secrets privilege
10 requires dismissal of the case. In *Halkin I*, for example, a number of individuals and
11 organizations claimed that they were subject to unlawful surveillance by the NSA and CIA
12 (among other agencies) due to their opposition to the Vietnam War. See 598 F.2d at 3. The D.C.

14
15 argument that the acquisition of a plaintiff's communications may be presumed from the
16 existence of a name on a watchlist, because "such a presumption would be unfair to the
individual defendants who would have no way to rebut it").

17 ⁹ (U) To the extent Plaintiffs challenge the TSP, see, e.g., Am. Compl. 32-37, their
18 allegations are insufficient on their face to establish standing even apart from the state secrets
19 issue because Plaintiffs fail to demonstrate that they fall anywhere near the scope of that
20 program. Plaintiffs do not claim to be, or to communicate with, members or affiliates of al
21 Qaeda—indeed, Plaintiffs expressly *exclude* from their purported class any foreign powers or
22 agents of foreign powers, "including without limitation anyone who knowingly engages in
23 sabotage or international terrorism, or activities that are in preparation therefore." Am. Compl.
24 ¶ 70. The named Plaintiffs thus are in no different position from any other citizen or AT&T
25 subscriber who falls *outside* the narrow scope of the TSP but nonetheless disagrees with the
26 program. Such a generalized grievance is clearly insufficient to support either constitutional or
27 prudential standing to challenge the TSP. See *Halkin II*, 690 F.2d at 1001-03 (holding that
28 individuals and organizations opposed to the Vietnam War lacked standing to challenge
intelligence activities because they did not adequately allege that they were (or immediately
would be) subject to such activities; thus, their claims were "nothing more than a generalized
grievance against the intelligence-gathering methods sanctioned by the President") (internal
quotation marks and citation omitted); *United Presbyterian Church v. Reagan*, 738 F.2d 1375,
1380 (D.C. Cir. 1984) (rejecting generalized challenge to alleged unlawful surveillance). To the
extent Plaintiffs allege classified intelligence activities beyond the TSP, Plaintiffs could not
prove such allegations in light of the state secrets assertion.

MEMORANDUM OF THE UNITED STATES IN SUPPORT
OF STATE SECRETS PRIVILEGE AND MOTION TO DISMISS
OR, IN THE ALTERNATIVE, FOR SUMMARY JUDGMENT
CASE NO. C-06-0672-VRW

1 Circuit upheld an assertion of the state secrets privilege regarding the identities of individuals
2 subject to NSA surveillance, rejecting the plaintiffs' argument that the privilege could not extend
3 to the "mere fact of interception," *id.* at 8, and despite significant public disclosures about the
4 surveillance activities at issue, *id.* at 10.¹⁰ A similar state secrets assertion with respect to the
5 identities of individuals subject to CIA surveillance was upheld in *Halkin II*. See 690 F.2d at
6 991. As a result of these privilege assertions in both *Halkin I* and *Halkin II*, the D.C. Circuit held
7 that the plaintiffs were incapable of demonstrating that they had standing to challenge the alleged
8 surveillance. See *id.* at 997.¹¹ Significantly, the court held that the fact of such surveillance
9 could not be proven even if the CIA had actually requested NSA to intercept the plaintiffs'
10 communications by including their names on a "watchlist" sent to NSA—a fact which was not
11 covered by the state secrets assertion in that case. See *id.* at 999-1000 ("[T]he absence of proof
12 of actual acquisition of appellants' communications is fatal to their watchlisting claims."). The
13 court thus found dismissal warranted, even though the complaint alleged actual interception of
14
15
16

17 ¹⁰ (U) As the court of appeals recognized, the "identification of the individuals or
18 organizations whose communications have or have not been acquired presents a reasonable
19 danger that state secrets would be revealed . . . [and] can be useful information to a sophisticated
intelligence analyst." *Halkin I*, 598 F.2d at 9.

20 ¹¹ (U) See *Halkin II*, 690 F.2d at 998 ("We hold that appellants' inability to adduce proof
21 of actual acquisition of their communications now prevents them from stating a cognizable claim
22 in the federal courts. In particular, we find appellants incapable of making the showing
23 necessary to establish their standing to seek relief."); *id.* at 997 (quoting district court's ruling
24 that "plaintiffs cannot show any injury from having their names submitted to NSA because NSA
25 is prohibited from disclosing whether it acquired any of plaintiffs' communications"); *id.* at 990
26 ("Without access to the facts about the identities of particular plaintiffs who were subjected to
27 CIA surveillance (or to NSA interception at the instance of the CIA), direct injury in fact to any
28 of the plaintiffs would not have been susceptible of proof."); *id.* at 987 ("Without access to
documents identifying either the subjects of . . . surveillance or the types of surveillance used
against particular plaintiffs, the likelihood of establishing injury in fact, causation by the
defendants, violations of substantive constitutional provisions, or the quantum of damages was
clearly minimal."); *Halkin I*, 598 F.2d at 7 ("[T]he acquisition of the plaintiffs' communication is
a fact vital to their claim," and "[n]o amount of ingenuity of counsel . . . can outflank the
Government's objection that disclosure of this fact is protected by privilege.").

1 plaintiffs' communications, because the plaintiffs' alleged injuries could be no more than
2 speculative in the absence of their ability to prove that such interception occurred. *Id.* at 999,
3 1001.¹²

4 (U) Similarly, in *Ellsberg v. Mitchell*, 709 F.2d 51 (D.C. Cir. 1983), a group of
5 individuals filed suit after learning during the course of the "Pentagon Papers" criminal
6 proceedings that one or more of them had been subject to warrantless electronic surveillance.
7 Although two such wiretaps were admitted, the Attorney General asserted the state secrets
8 privilege, refusing to disclose to the plaintiffs whether any other such surveillance occurred. *See*
9 *id.* at 53-54. As a result of the privilege assertion, the court upheld the district court's dismissal
10 of the claims brought by the plaintiffs the Government had not admitted overhearing, because
11 those plaintiffs could not prove actual injury. *See id.* at 65.

14 (U) The same result is required here. In light of the state secrets assertion, Plaintiffs
15 cannot prove that their communications were intercepted or disclosed by AT&T, and thus they
16 cannot meet their burden to establish standing. Accordingly, like other similar cases before it,
17 this action must be dismissed.¹³

19
20 ¹² (U) Because the CIA conceded that nine plaintiffs were subjected to certain types of
21 non-NSA surveillance, the D.C. Circuit held that those plaintiffs had demonstrated an injury-in-
22 fact. *See Halkin II*, 690 F.2d at 1003. Nonetheless, the nine plaintiffs were precluded from
23 seeking injunctive and declaratory relief because they could not demonstrate the likelihood of
future injury or a live controversy in light of the fact that the CIA had terminated the specific
intelligence methods at issue. *See id.* at 1005-09.

24 ¹³ (U) Plaintiffs cannot overcome this fundamental standing bar simply by alleging that
25 their speech has been chilled as the result of their own subjective fear of Government
26 surveillance. *See Plaintiffs' Memorandum of Points and Authorities in Support of Motion for*
27 *Preliminary Injunction* at 25. Specifics about this alleged chilling effect are provided with
28 respect to only one plaintiff, Carolyn Jewel, who claims that she has refrained from responding
openly about Islam or U.S. foreign policy in e-mails to a Muslim individual in Indonesia, and
that she has decided against using the Internet to conduct certain research for her action and
futuristic romance novels. *See id.* at 26. Plaintiffs offer no explanation as to how this admitted

MEMORANDUM OF THE UNITED STATES IN SUPPORT
OF STATE SECRETS PRIVILEGE AND MOTION TO DISMISS
OR, IN THE ALTERNATIVE, FOR SUMMARY JUDGMENT
CASE NO. C-06-0672-VRW

1 [REDACTED TEXT]

2 2. (U) Plaintiffs' Statutory Claims Cannot Be
3 Proven or Defended Without State Secrets.

4 [REDACTED TEXT]

5 (U) To prove their FISA claim (as alleged in Count I), Plaintiffs would have to show that
6 AT&T intentionally acquired, under color of law and by means of a surveillance device within
7 the United States, the contents of one or more wire communications to or from Plaintiffs. *See*
8 *Am Compl.* ¶¶ 93–94; 50 U.S.C. §§ 1801(f), 1809, 1810. Likewise, to prove their claim under
9 18 U.S.C. § 2511 (as alleged in Count III), Plaintiffs would have to demonstrate that AT&T
10 intentionally intercepted, disclosed, used, and/or divulged the contents of Plaintiffs' wire or
11 electronic communications. *See Am. Compl.* ¶¶ 102–07. Plaintiffs' claims under 47 U.S.C.
12 § 605, 18 U.S.C. § 2702, and Cal. Bus. & Prof. Code §§ 17200, *et seq.*, all require similar proof:
13 the acquisition and/or disclosure of Plaintiffs' communications and related information. Any
14 information tending to confirm or deny the alleged activities, or any alleged AT&T involvement,
15 is subject to the state secrets privilege.
16
17

18 (U) In addition to proving actual interception or disclosure to the NSA of their
19 communications, Plaintiffs must also prove, for each of their statutory claims, that any alleged
20 interception or disclosure was not authorized by the Government. In particular, 18 U.S.C.
21 § 2511(2)(a)(ii) provides:
22
23

24 “self-censorship” makes any sense in light of the acknowledged limitation of the TSP to
25 international communications actually conducted by al Qaeda-affiliated individuals, as opposed
26 to a mass targeting of particular *topics* of conversation or research. *Id.* In any event, Plaintiffs'
27 claim of a chilling effect is foreclosed by *Laird v. Tatum*, 408 U.S. 1 (1972), which squarely
28 rejected the assertion of a subjective chill caused by the mere existence of an intelligence
program as a basis to challenge that program. *See* 408 U.S. at 13–14 (“Allegations of a
subjective chill are not an adequate substitute for a claim of specific present objective harm or a
threat of specific future harm.”) (internal quotation marks omitted).

MEMORANDUM OF THE UNITED STATES IN SUPPORT
OF STATE SECRETS PRIVILEGE AND MOTION TO DISMISS
OR, IN THE ALTERNATIVE, FOR SUMMARY JUDGMENT
CASE NO. C-06-0672-VRW

1 Notwithstanding any other law, providers of wire or electronic communication
2 service, their officers, employees, and agents, landlords, custodians, or other
3 persons, are authorized to provide information, facilities, or technical assistance to
4 persons authorized by law to intercept wire, oral, or electronic communications or
5 to conduct electronic surveillance, as defined in section 101 of the Foreign
6 Intelligence Surveillance Act of 1978, if such provider, its officers, employees, or
7 agents, landlord, custodian, or other specified person, has been provided with—
8 (A) a court order directing such assistance signed by the authorizing judge, or
9 (B) a certification in writing by a person specified in section 2518(7) of this title or
10 the Attorney General of the United States that no warrant or court order is
11 required by law, that all statutory requirements have been met, and that the
12 specified assistance is required.

13 (U) If a court order or Government certification is provided, the telecommunications
14 provider is absolutely immune from liability in any case:

15 No cause of action shall lie in any court against any provider of wire or electronic
16 communication service, its officers, employees, or agents, landlord, custodian, or
17 other specified person for providing information, facilities, or assistance in
18 accordance with the terms of a court order or certification under this chapter.

19 18 U.S.C. § 2511(2)(a)(ii).¹⁴

20 (U) As AT&T has correctly explained, the absence of a court order or Government
21 certification under section 2511(2)(a)(ii) is an element of Plaintiffs' claims. *See* AT&T's Motion
22 to Dismiss Amended Complaint at 7-8. Thus, Plaintiffs bear the burden of alleging and proving
23 the lack of such authorization. *See* Senate Report No. 99-541, reprinted in 1986 U.S.C.C.A.N.
24 3555, 3580 (1986) (stating that a plaintiff "must allege" the absence of a court order or
25 certification; otherwise "the defendant can move to dismiss the complaint for failure to state a
26 claim upon which relief can be granted"). Notably, Plaintiffs fail to meet that burden on the face
27 of their pleadings; they do not specifically allege that AT&T, if it assisted with any alleged

28 ¹⁴ (U) *See also, e.g.*, 18 U.S.C. § 2703(e) (same); 50 U.S.C. § 1809 (prohibiting
electronic surveillance under color of law "except as authorized by statute"); 18 U.S.C.
§ 2511 (prohibiting intercepts "[e]xcept as otherwise specifically provided in this chapter").

1 activity, acted without Government authorization. This action may be dismissed on that basis
2 alone. *See* AT&T's Motion to Dismiss Amended Complaint at 7-8. But even if Plaintiffs
3 speculated and alleged the absence of section 2511(2)(a)(ii) authorization, they could not meet
4 their burden of proof on the issue because information confirming or denying AT&T's
5 involvement in alleged intelligence activities is covered by the state secrets assertion.

6
7 [REDACTED TEXT]

8 **3. (U) Plaintiffs' Fourth Amendment Claim Cannot Be Adjudicated**
9 **Without State Secrets**

10 (U) Plaintiffs' Fourth Amendment claim also cannot be proven or defended without
11 information covered by the state secrets assertion. Specifically, Plaintiffs allege that they have a
12 reasonable expectation of privacy in the contents of, and records pertaining to, their
13 communications, and that their rights were violated when AT&T allegedly intercepted or
14 disclosed such communications and records at the instigation of the Government and without
15 lawful authorization. *See* Am. Compl. ¶¶ 78-89.

16
17 (U) In their preliminary injunction motion, which is focused on Internet communications,
18 Plaintiffs further claim that, "[a]s an agent of the Government," AT&T is engaged in "wholesale
19 copying of vast amounts of communications carried by its WorldNet Internet service." *Pls.*
20 *Prelim. Inj. Mem.* at 25. Plaintiffs assert that the alleged surveillance violates the Fourth
21 Amendment because it involves "an automated 'rummaging' through the millions of private
22 communications passing over AT&T's fiber optic network at the discretion of NSA staff." *See*
23 *id.* at 27. Plaintiffs simply assume that a warrant is required for any and all of the surveillance
24 activities alleged in their Complaint. *See id.*

25
26
27 [REDACTED TEXT]

28 (U) The requirement of a warrant supported by probable cause is not universal but turns

1 on the particular circumstances at issue. The Supreme Court has made clear that, while a search
2 must be supported, as a general matter, by a warrant issued upon probable cause, it has
3 repeatedly “reaffirm[ed] a longstanding principle that neither a warrant nor probable cause, nor,
4 indeed, any measure of individualized suspicion, is an indispensable component of
5 reasonableness in every circumstance.” *National Treasury Employees Union v. Von Raab*, 489
6 U.S. 656, 665 (1989).

8 (U) For example, both before and after the enactment of the Foreign Intelligence
9 Surveillance Act, every federal appellate court to consider the issue has concluded that, even in
10 peacetime, the President has inherent constitutional authority, consistent with the Fourth
11 Amendment, to conduct searches for foreign intelligence purposes without securing a judicial
12 warrant. *See In re Sealed Case*, 310 F.3d 717, 742 (Foreign Intel. Surv. Ct. of Rev. 2002) (“[A]ll
13 the other courts to have decided the issue [have] held that the President did have inherent
14 authority to conduct warrantless searches to obtain foreign intelligence information *We take*
15 *for granted that the President does have that authority and, assuming that is so, FISA could not*
16 *encroach on the President’s constitutional power.”) (emphasis added); accord, e.g., *United*
17 *States v. Truong Dinh Hung*, 629 F.2d 908 (4th Cir. 1980); *United States v. Butenko*, 494 F.2d
18 593 (3d Cir. 1974) (en banc); *United States v. Brown*, 484 F.2d 418 (5th Cir. 1973). *But cf.*
19 *Zweibon v. Mitchell*, 516 F.2d 594 (D.C. Cir. 1975) (en banc) (dictum in plurality opinion
20 suggesting that a warrant would be required even in a foreign intelligence investigation).*

21 (U) In *United States v. United States District Court*, 407 U.S. 297 (1972) (“*Keith*”), the
22 Supreme Court concluded that the Fourth Amendment’s warrant requirement applies to
23 investigations of wholly *domestic* threats to security—such as domestic political violence and
24 other crimes. But the Court made clear that it was not addressing the President’s authority to
25
26
27
28

1 conduct *foreign* intelligence surveillance (even within the United States) without a warrant and
2 that it was expressly reserving that question: “[T]he instant case requires no judgment on the
3 scope of the President’s surveillance power with respect to the activities of foreign powers,
4 within or without this country.” *Id.* at 308; *see also id.* at 321-22 & n.20 (“We have not
5 addressed, and express no opinion as to, the issues which may be involved with respect to
6 activities of foreign powers or their agents.”).¹⁵ That *Keith* does not apply in the context of
7 protecting against a foreign attack has been confirmed by the lower courts. After *Keith*, each of
8 the three courts of appeals that have squarely considered the question has concluded—expressly
9 taking the Supreme Court’s decision into account—that the President has inherent authority to
10 conduct warrantless surveillance in the foreign intelligence context. *See, e.g., Truong Dinh*
11 *Hung*, 629 F.2d at 913-14; *Butenko*, 494 F.2d at 603; *Brown*, 484 F.2d 425-26. As one court put
12 it:

13
14
15 [F]oreign intelligence gathering is a clandestine and highly unstructured activity,
16 and the need for electronic surveillance often cannot be anticipated in advance.
17 Certainly occasions arise when officers, acting under the President’s authority, are
18 seeking foreign intelligence information, where exigent circumstances would
19 excuse a warrant. To demand that such officers be so sensitive to the nuances of
20 complex situations that they must interrupt their activities and rush to the nearest
21 available magistrate to seek a warrant would seriously fetter the Executive in the
22 performance of his foreign affairs duties.

23
24
25 ¹⁵ (U) *Keith* made clear that one of the significant concerns driving the Court’s
26 conclusion in the domestic security context was the inevitable connection between perceived
27 threats to domestic security and political dissent. As the Court explained: “Fourth Amendment
28 protections become the more necessary when the targets of official surveillance may be those
suspected of unorthodoxy in their political beliefs. The danger to political dissent is acute where
the Government attempts to act under so vague a concept as the power to protect ‘domestic
security.’” *Keith*, 407 U.S. at 314; *see also id.* at 320 (“Security surveillances are especially
sensitive because of the inherent vagueness of the domestic security concept, the necessarily
broad and continuing nature of intelligence gathering, and the temptation to utilize such
surveillances to oversee political dissent.”). Surveillance of domestic groups raises a First
Amendment concern that generally is not present when the subjects of the surveillance are
foreign powers or their agents.

1 *Butenko*, 494 F.2d 605.

2
3 (U) Beyond this, the Supreme Court has held that the warrant requirement is inapplicable
4 in situations involving "special needs" that go beyond a routine interest in law enforcement.
5 *Vernonia Sch. Dist. v. Acton*, 515 U.S. 646, 653 (1995) (there are circumstances "when special
6 needs, beyond the normal need for law enforcement, make the warrant and probable-cause
7 requirement impracticable") (quoting *Griffin v. Wisconsin*, 483 U.S. 868, 873 (1987)); *Illinois v.*
8 *McArthur*, 531 U.S. 326, 330 (2001) ("When faced with special law enforcement needs,
9 diminished expectations of privacy, minimal intrusions, or the like, the Court has found that
10 certain general, or individual, circumstances may render a warrantless search or seizure
11 reasonable."). One application in which the Court has found the warrant requirement
12 inapplicable is in circumstances in which the Government faces an increased need to be able to
13 react swiftly and flexibly, or interests in public safety beyond the interests in ordinary law
14 enforcement are at stake. See, e.g., *Skinner v. Railway Labor Executives' Ass'n*, 489 U.S. 602,
15 634 (1989) (drug testing of railroad personnel involved in train accidents). As should be
16 apparent, demonstrating that this body of law applies to a particular case requires reference to
17 specific facts.
18
19
20

21 [REDACTED TEXT]

22 (U) Beyond the warrant requirement, analysis of Plaintiffs' Fourth Amendment claim
23 requires a fact-intensive inquiry regarding whether a particular search satisfies the Fourth
24 Amendment's "central requirement . . . of reasonableness." *McArthur*, 531 U.S. at 330; see also
25 *Board of Educ. v. Earls*, 536 U.S. 822, 828 (2002). What is reasonable, of course, "depends on
26 all of the circumstances surrounding the search or seizure and the nature of the search or seizure
27
28

1 itself." *United States v. Montoya de Hernandez*, 473 U.S. 531, 537 (1985). Thus, the
2 permissibility of a particular practice "is judged by balancing its intrusion on the individual's
3 Fourth Amendment interests against its promotion of legitimate Governmental interests."
4 *Delaware v. Prouse*, 440 U.S. 648, 654 (1979).

5 [REDACTED TEXT]

6
7 (U) Indeed, in specifically addressing a Fourth Amendment challenge to warrantless
8 electronic surveillance, the court in *Halkin II* observed that "the focus of the proceedings would
9 necessarily be upon 'the "reasonableness" of the search and seizure in question.'" 690 F.2d at
10 1001 (citing *Keith*, 407 U.S. at 308). "The valid claim of the state secrets privilege makes
11 consideration of that question impossible." *Id.* Without evidence of the detailed circumstances
12 in which alleged surveillance activities were being conducted—that is, without "the essential
13 information on which the legality of executive action (in foreign intelligence surveillance)
14 turns"—the court in *Halkin II* held that "it would be inappropriate to resolve the extremely
15 difficult and important fourth amendment issue presented." *Id.*¹⁶ This holding fully applies here.

16 [REDACTED TEXT]

17
18 (U) None of these issues can be decided on the limited, incomplete public record of what
19 has been disclosed about the Terrorist Surveillance Program. Any effort to determine the
20 reasonableness of allegedly warrantless foreign intelligence activities under such conditions
21 "would be tantamount to the issuance of an advisory opinion on the question." *Halkin II*, 690
22 F.2d at 1001 (citing *Chagnon v. Bell*, 642 F.2d 1248, 1263 (D.C. Cir. 1980)). In sum, the
23
24
25

26
27 ¹⁶ (U) See also *Halkin II*, 690 F.2d at 1000 ("Determining the reasonableness of
28 warrantless foreign intelligence watchlisting under conditions of such informational poverty [due
to the state secrets assertion] . . . would be tantamount to the issuance of an advisory opinion on
the question.").

1 lawfulness of the alleged activities cannot be determined without a full factual record, and that
2 record cannot be made in civil litigation without seriously compromising U.S. national security
3 interests.

4 **4. (U) Whether Alleged Surveillance Activities Are Properly Authorized**
5 **by Law Cannot be Resolved without State Secrets.**

6 (U) Finally, in addition to all of the foregoing issues that could not be litigated
7 without the disclosure of state secrets, adjudication of whether the alleged surveillance activities
8 have been conducted within lawful authority cannot be resolved without state secrets. Plaintiffs
9 allege "that the Program's surveillance has been conducted without Court orders" for several
10 years, and that it involves "the wholesale, long-term interception of customer communications
11 seen here." Pls. Prelim. Inj. Mem. at 20. Plaintiffs also seek to address whether the Government
12 certified to AT&T, pursuant to the statutory provisions on which Plaintiffs have based their
13 claims, the lawfulness of the alleged activities, *see id.* n. 23, and whether AT&T's reliance on
14 any such certification would have been reasonable. *Id.* at 21. And Plaintiffs put at issue (as a
15 general matter) those situations in which warrantless wiretapping may lawfully occur. *Id.* at 20-
16 21. Again quite clearly, Plaintiffs' allegations put at issue the factual basis of the alleged
17 activities.
18

19 [REDACTED TEXT]
20

21 (U) Litigation regarding Plaintiffs' claim that the President has acted in excess of his
22 authority also would require an exposition of the scope, nature, and kind of the alleged activities.
23 It is well-established that, pursuant to his authority under Article II of the Constitution as
24 Commander-in-Chief, the President's most basic constitutional duty is to protect the Nation from
25 armed attack. *See, e.g., The Prize Cases*, 67 U.S. 635, 668 (1862); *see generally Ex parte*
26 *Quirin*, 317 U.S. 1, 28 (1942). It is also well-established that the President may exercise his
27

1 statutory and constitutional authority to gather intelligence information about foreign enemies.
2 *See, e.g., Totten v. United States*, 92 U.S. 105, 106 (1876) (recognizing President's authority to
3 hire spies); *see also Chicago & S. Air Lines v. Waterman S.S. Corp.*, 333 U.S. 103, 111 (1948)
4 ("The President, both as Commander-in-Chief and as the Nation's organ for foreign affairs, has
5 available intelligence services whose reports neither are not and ought not to be published to the
6 world."); *United States v. Curtiss-Wright Export Corp.*, 299 U.S. 304, 320 (1936) (The President
7 "has his confidential sources of information. He has his agents in the form of diplomatic,
8 consular, and other officials."). And, as noted, courts have held that the President has inherent
9 constitutional authority to authorize foreign intelligence surveillance. *See supra*.

10
11 [REDACTED TEXT]

12
13 **(U) CONCLUSION**

14 For the foregoing reasons, the Court should:

15
16 1. Uphold the United States' assertion of the military and state secrets privilege and
17 exclude from this case the information identified in the Declarations of John D. Negroponte,
18 Director of National Intelligence of the United States, and Keith B. Alexander, Director of the
19 National Security Agency; and

20
21 2. Dismiss this action because adjudication of Plaintiffs' claims risks or requires the
22 disclosure of protected state secrets and would thereby risk or cause exceptionally grave harm to
23 the national security of the United States.
24
25
26
27
28

1 Respectfully submitted,

2 PETER D. KEISLER
3 Assistant Attorney General

4 CARL J. NICHOLS
5 Deputy Assistant Attorney General

6 DOUGLAS N. LETTER
7 Terrorism Litigation Counsel

8 JOSEPH H. HUNT
9 Director, Federal Programs Branch

10 *s/ Anthony J. Coppolino*
11 ANTHONY J. COPPOLINO
12 Special Litigation Counsel
13 tony.coppolino@usdoj.gov

14 *s/ Andrew H. Tannenbaum*
15 ANDREW H. TANNENBAUM
16 Trial Attorney
17 andrew.tannenbaum@usdoj.gov
18 U.S. Department of Justice
19 Civil Division, Federal Programs Branch
20 20 Massachusetts Avenue, NW
21 Washington, D.C. 20001
22 Phone: (202) 514-4782/(202) 514-4263
23 Fax: (202) 616-8460/(202) 616-8202

24 Attorneys for United States of America

25 DATED: May 12, 2006

26
27
28 MEMORANDUM OF THE UNITED STATES IN SUPPORT
OF STATE SECRETS PRIVILEGE AND MOTION TO DISMISS
OR, IN THE ALTERNATIVE, FOR SUMMARY JUDGMENT
CASE NO. C-06-0672-VRW

CERTIFICATE OF SERVICE

I hereby certify that the foregoing NOTICE OF MOTION AND MOTION TO DISMISS OR, IN THE ALTERNATIVE, FOR SUMMARY JUDGMENT BY THE UNITED STATES OF AMERICA will be served by means of the Court's CM/ECF system, which will send notifications of such filing to the following:

Electronic Frontier Foundation
Cindy Cohn
Lee Tien
Kurt Opsahl
Kevin S. Bankston
Corynne McSherry
James S. Tyre
545 Shotwell Street
San Francisco, CA 94110

Lerach Coughlin Stoia Geller Rudman & Robbins LLP
Reed R. Kathrein
Jeff D. Friedman
Shana E. Scarlett
100 Pine Street, Suite 2600
San Francisco, CA 94111

Traber & Voorhees
Bert Voorhees
Theresa M. Traber
128 North Fair Oaks Avenue, Suite 204
Pasadena, CA 91103

Pillsbury Winthrop Shaw Pittman LLP
Bruce A. Ericson
David L. Anderson
Patrick S. Thompson
Jacob R. Sorensen
Brian J. Wong
50 Freemont Street
PO Box 7880
San Francisco, CA 94120-7880

Sidney Austin LLP
David W. Carpenter
Bradford Berenson
Edward R. McNicholas
David L. Lawson
1501 K Street, NW
Washington, DC 20005

s/ Anthony J. Coppolino

EXHIBIT E

1 PETER D. KEISLER
 Assistant Attorney General, Civil Division
 2 CARL J. NICHOLS
 Deputy Assistant Attorney General
 3 DOUGLAS N. LETTER
 Terrorism Litigation Counsel
 4 JOSEPH H. HUNT
 Director, Federal Programs Branch
 5 ANTHONY J. COPPOLINO
 Special Litigation Counsel
 6 tony.coppolino@usdoj.gov
 RENÉE S. ORLEANS
 7 renee.orleans@usdoj.gov
 ANDREW H. TANNENBAUM
 8 andrew.tannenbaum@usdoj.gov
 Trial Attorneys
 9 U.S. Department of Justice
 Civil Division, Federal Programs Branch
 10 20 Massachusetts Avenue, NW
 Washington, D.C. 20001
 11 Phone: (202) 514-4782/(202) 514-4263
 Fax: (202) 616-8460/(202) 616-8202/(202) 318-2461

12 Attorneys for Intervenor Defendant United States of America

13 UNITED STATES DISTRICT COURT
 14 NORTHERN DISTRICT OF CALIFORNIA
 15

16 TASH HEPTING, GREGORY HICKS)
 17 CAROLYN JEWEL and ERIK KNUTZEN)
 on Behalf of Themselves and All Others)
 18 Similarly Situated,)

19 Plaintiffs,)

20 v.)

21 AT&T CORP., AT&T INC. and)
 DOES 1-20, inclusive,)

22 Defendants.)
 23)
 24)
 25)
 26)
 27)
 28)

Case No. C-06-0672-VRW

**UNITED STATES' RESPONSE
 TO PLAINTIFFS' MEMORANDUM
 OF POINTS AND AUTHORITIES
 IN RESPONSE TO COURT'S MAY 17,
 2006 MINUTE ORDER**

TABLE OF CONTENTS

1
2 INTRODUCTION 1
3 ARGUMENT 2
4 I. *IN CAMERA, EX PARTE* REVIEW OF THE UNITED STATES' SUBMISSIONS
5 DOES NOT VIOLATE DUE PROCESS. 2
6 II. PLAINTIFFS ARE NOT ENTITLED TO ACCESS TO THE CLASSIFIED
7 MATERIALS SUBMITTED *IN CAMERA, EX PARTE*. 8
8 III. PLAINTIFFS HAVE OFFERED NO VALID REASON FOR THE COURT TO
9 FOREGO REVIEW OF THE *IN CAMERA, EX PARTE* MATERIALS. 13
10 CONCLUSION 20
11 CERTIFICATE OF SERVICE

TABLE OF AUTHORITIES

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

CASES

American-Arab Anti-Discrim. Comm. v. Reno,
70 F.3d 1045 (9th Cir. 1995) 5

Armstrong v. Bush,
924 F.2d 282 (D.C. Cir. 1991) 13

Central Intelligence Agency v. Sims,
471 U.S. 159 (1985) 5

City of Los Angeles v. Lyons,
461 U.S. 95 (1983) 14

DTM Research, L.L.C. v. AT&T Corp.,
245 F.3d 327 (4th Cir. 2001) 10

Dept. of Navy v. Egan,
484 U.S. 518 (1988) 5, 9, 13

Doe v. Browner,
902 F. Supp. 1240 (D. Nev. 1995) 4

Dorfmont v. Brown,
913 F.2d 1399 (9th Cir. 1990) 9

Edmonds v. U.S. Dept. of Justice,
323 F. Supp. 2d 65 (D.D.C. 2004),
aff'd, 161 Fed. Appx. 6 (D.C. Cir.),
cert. denied, 126 S. Ct. 734 (2005) 4, 19

El Masri v. Tenet,
Civil Action No. 05-1417 (E.D. Va.) passim

Ellsberg v. Mitchell,
709 F.2d 51 (D.C. Cir. 1983) 17, 20

Fitzgerald v. Penthouse Int'l, Ltd.,
776 F.2d 1236 (4th Cir. 1985) 14, 16

Gilbert v. Homar,
520 U.S. 924 (1997) 6

Global Relief Found. v. O'Neill,
315 F.3d 748 (7th Cir. 2002), *cert. denied*, 540 U.S. 1003 (2003) 4

In re Grand Jury Proceedings,
867 F.2d 539 (9th Cir. 1988) 3

1 *Guenther v. Comm'r of Internal Revenue*,
889 F.2d 882 (9th Cir. 1989) 3, 7

2

3 *Haig v. Agee*,
453 U.S. 280 (1981) 3, 5

4 *Halkin v. Helms*,
598 F.2d 1 (D.C. Cir. 1978) 11, 18

5

6 *Halkin v. Helms*,
690 F.2d 977 (D.C. Cir. 1982) 15, 16, 18

7 *Hayden v. Nat'l Security Agency*,
608 F.2d 1381 (D.C. Cir. 1979) 10

8

9 *Holy Land Found. for Relief & Dev. v. Ashcroft*,
333 F.3d 156 (D.C. Cir. 2003),
cert. denied, 540 U.S. 1218 (2004) 4

10

11 *In re Sealed Case No. 98-3077*,
151 F.3d 1059 (D.C. Cir. 1998) 6

12 *In re Under Seal*,
945 F.2d 1285 (4th Cir. 1991) 18

13

14 *In re United States*,
1 F.3d 1251 10

15 *In re United States*,
872 F.2d 472 (D.C. Cir. 1989) 18

16

17 *Jifry v. Fed. Aviation Admin.*,
370 F.3d 1174 (D.C. Cir. 2004),
cert. denied, 543 U.S. 1146 (2005) 3

18

19 *Kasza v. Browner*,
133 F.3d 1159 (9th Cir. 1988) passim

20 *Lujan v. Defenders of Wildlife*,
504 U.S. 555 (1992) 12, 14

21

22 *Lynn v. Regents of Univ. of Calif.*,
656 F.2d 1337 (9th Cir. 1981) 7

23 *Meridian Int'l Logistics, Inc. v. United States*,
939 F.2d 740 (9th Cir. 1991) 2, 3, 6, 7

24

25 *Molerio v. Fed. Bureau of Investigation*,
749 F.2d 815 (D.C. Cir. 1984) 16

26 *Morrissey v. Brewer*,
408 U.S. 471 (1972) 6

27

1 *Nadarajah v. Gonzales*,
 443 F.3d 1069 (9th Cir. 2006) 12

2

3 *Nat'l Council of Resistance of Iran v. Dept. of State*,
 251 F.3d 192 (D.C. Cir. 2001) 6

4 *Nixon v. Sirica*,
 487 F.2d 700 (D.C. Cir. 1973) 18

5

6 *O'Shea v. Littleton*,
 414 U.S. 488 (1974) 14

7 *Patterson v. Fed. Bureau of Investigation*,
 893 F.2d 595 (3d Cir. 1990) 4

8

9 *People's Mojahedin Org. of Iran v. Dept. of State*,
 327 F.3d 1238 (D.C. Cir. 2003) 4, 10

10 *Pollard v. Fed. Bureau of Investigation*,
 705 F.2d 1151 (9th Cir. 1983) 3, 9

11

12 *Salisbury v. United States*,
 690 F.2d 966 (D.C. Cir. 1982) 4, 10, 18

13 *Snepp v. United States*,
 444 U.S. 507 (1980) 3

14

15 *Steel Co. v. Citizens for a Better Environment*,
 523 U.S. 83 (1998) 15

16 *Sterling v. Tenet*,
 416 F.3d 338 (4th Cir. 2005), *cert. denied*, 126 S. Ct. 1052 (2006) 4, 11

17

18 *Tenet v. Doe*,
 544 U.S. 1 (2005) 14

19 *Torbet v. United Airlines*,
 298 F.3d 1087 (9th Cir. 2002) 4

20

21 *Totten v. United States*,
 92 U.S. 105 (1875) 13, 14

22 *United Presbyterian Church in the U.S.A. v. Reagan*,
 738 F.2d 1375 (D.C. Cir. 1984) 15

23

24 *United States v. Badia*,
 827 F.2d 1458 (11th Cir. 1987) 12

25 *United States v. Belfield*,
 692 F.2d 141 (D.C. Cir. 1982) 12

26

27

1 *United States v. Duggan,*
743 F.2d 59 (2d Cir. 1984) 12

2

3 *United States v. Hamide,*
914 F.2d 1147 (9th Cir. 1990) 12

4 *United States v. Isa,*
923 F.2d 1300 (8th Cir. 1991) 12

5

6 *United States v. Johnson,*
952 F.2d 565 (1st Cir. 1991) 12

7 *United States v. Klimavicius-Viloria,*
144 F.3d 1249 (9th Cir. 1998) 8

8

9 *United States v. Ott,*
827 F.2d 473 (9th Cir. 1987) 3, 12

10 *United States v. Reynolds,*
345 U.S. 1 (1953) 17

11

12 *United States v. Squillacote,*
221 F.3d 542 (4th Cir. 2000) 12

13 *United States v. Thompson,*
827 F.2d 1254 (9th Cir. 1987) 8

14

15 *Wayte v. United States,*
470 U.S. 598 (1985)

16 *Weberman v. Nat'l Security Agency,*
668 F.2d 676 (2d Cir. 1982) 10

17

18 **STATUTES**

19 Cal. Bus. & Prof. Code §§ 17200, *et seq* 16

20 18 U.S.C. § 2511 16

21 47 U.S.C. § 605, 18 U.S.C. § 2702 16

22 47 U.S.C. § 2511(2) 17

23 50 U.S.C. § 402 12

24 50 U.S.C. § 1801 *et seq* passim

25 50 U.S.C. § 1806(f) 9, 11, 12

26 50 U.S.C. § 1809 16

27

1 50 U.S.C. § 1810 16
2 50 U.S.C. § 1845(f) 9

3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

1 INTRODUCTION

2 In this case, the United States has invoked the military and state secrets privilege
3 (hereinafter “state secrets privilege”) to protect information which two of the nation’s highest
4 ranking intelligence officials have determined cannot be disclosed without causing harm to the
5 national security interests of the United States. On the basis of determinations made by the
6 Director of National Intelligence and the Director of the National Security Agency, the United
7 States has explained in public filings and, in more detail, in filings submitted for the Court’s *in*
8 *camera, ex parte* review, why no aspect of this case can be litigated without disclosing state
9 secrets. The United States has not lightly invoked the state secrets privilege, and the weighty
10 reasons for asserting the privilege are apparent from the classified material submitted in support
11 of its assertion. The need to protect against the harm to national security that would arise from
12 the disclosure of classified information, however, makes it impossible for the United States to
13 explain on the public record more precisely what those reasons are. Although the Court could
14 dismiss this action based on the public filings already made, in light of the grave national security
15 implications at issue in this case, it would be perilous to proceed instead to litigate any of
16 Plaintiffs’ claims here without full consideration of the details of the Government’s state secrets
17 privilege assertion, including the material that the United States has submitted for this Court’s *in*
18 *camera, ex parte* review.

19 Plaintiffs argue that consideration by the Court of the *in camera, ex parte* evidence
20 submitted by the United States can deprive them of due process; that the Foreign Intelligence
21 Surveillance Act (“FISA”) requires them to be provided with access to the underlying materials;
22 and that the Court should not review the *in camera, ex parte* materials submitted by the United
23 States, but should instead allow Plaintiffs certain discovery and address Plaintiffs’ legal claims
24 based on the information available on the public record. Each of these arguments is misguided.
25 It is well established that where classified materials are at issue, a court may review such material
26 *in camera, ex parte* without infringing a litigant’s due process rights in order to avoid the harms
27

1 that would result from unauthorized disclosure. Moreover, neither FISA nor any other provision
2 of law can be construed to provide Plaintiffs with access either to classified material subject to
3 the state secrets privilege or to material subject to the statutory privileges invoked by the United
4 States.

5 Finally, Plaintiffs' belief that the Court should defer review of the United States' *in*
6 *camera, ex parte* submissions because Plaintiffs can prove their *prima facie* case based on
7 materials available in the public record, and that they are entitled to certain discovery in their
8 effort to do so, reflects a fundamental misconception of the scope, nature and effect of the
9 Government's invocation of the state secrets privilege. As described in the United States' public
10 filing and in the supporting classified materials, state secrets are central to the Plaintiffs'
11 allegations and any attempt to proceed with the litigation will threaten the disclosure of
12 privileged matters. Because, for the reasons explained in the Government's earlier submissions,
13 including in the public Memorandum of the United States in Support of the Military and State
14 Secrets Privilege and Motion to Dismiss or, in the Alternative, for Summary Judgment, Docket
15 No. 124 ("U.S. Mem."), Plaintiffs cannot prove their *prima facie* case without resort to classified
16 material, the Court should consider the dispositive motions of the United States and AT&T
17 before taking any further action in this case.

18 **ARGUMENT**

19 **I. *IN CAMERA, EX PARTE* REVIEW OF THE UNITED STATES' SUBMISSIONS**
20 **DOES NOT VIOLATE DUE PROCESS.**

21 Plaintiffs' initial argument is that due process disfavors the Court's consideration of
22 materials provided *in camera* and *ex parte*. Although *ex parte* submissions are not the norm,
23 courts have repeatedly recognized that such submissions are necessary in a variety of contexts.
24 *See, e.g., Meridian Int'l Logistics, Inc. v. United States*, 939 F.2d 740, 745 (9th Cir. 1991) ("We
25 find that the procedure [declarations sealed and subject to *in camera, ex parte* review] used by
26 the court in the instant case was proper; it adequately balanced the rights of the Government and
27 [plaintiff]. . . . [A]lthough [plaintiff] did not have the opportunity to conduct discovery and

1 cross-examine the Government's witness, its interests as a litigant are satisfied by the ex parte/in
2 camera decision of an impartial district judge."); *In re Grand Jury Proceedings*, 867 F.2d 539,
3 540-41 (9th Cir. 1988) (rejecting due process challenge to *in camera* submission supporting
4 enforcement of grand jury subpoena); *United States v. Ott*, 827 F.2d 473, 476-77 (9th Cir. 1987)
5 (rejecting due process challenge to *in camera, ex parte* review of materials under the Foreign
6 Intelligence Surveillance Act, 50 U.S.C. § 1801 *et seq.*); *Pollard v. Fed. Bureau of Investigation*,
7 705 F.2d 1151, 1153-54 (9th Cir. 1983) ("the practice of *in camera, ex parte* review remains
8 appropriate in certain [Freedom of Information Act ("FOIA")] cases").

9 More specifically, as the Court of Appeals squarely recognized in the very case upon
10 which Plaintiffs predominately rely, *in camera, ex parte* submissions are appropriate when there
11 is "some 'compelling justification.'" *Guenther v. Comm'r of Internal Revenue*, 889 F.2d 882,
12 884 (9th Cir. 1989) ("*Guenther I*"), *appeal decided after remand by*, 939 F.2d 758 (9th Cir.
13 1991) ("*Guenther II*") (quoting *United States v. Thompson*, 827 F.2d 1254, 1258-59 (9th Cir.
14 1986)). "It is 'obvious and unarguable' that no governmental interest is more compelling than
15 the security of the Nation." *Haig v. Agee*, 453 U.S. 280, 307 (1981) (citation omitted); *see also*
16 *Wayte v. United States*, 470 U.S. 598, 612 (1985) ("Unless a society has the capability and will to
17 defend itself from the aggressions of others, constitutional protections of any sort will have little
18 meaning"); *Snepp v. United States*, 444 U.S. 507, 509 n.3 (1980) ("The Government has a
19 compelling interest in protecting both the secrecy of information important to our national
20 security and the appearance of confidentiality so essential to the effective operation of our foreign
21 intelligence service.").

22 Thus, numerous courts have considered *in camera, ex parte* submissions containing
23 information that is classified or that relates to ongoing counter-terrorism efforts of the federal
24 government, and have rejected due process challenges to such a course. *See, e.g., Jifry v. Fed.*
25 *Aviation Admin.*, 370 F.3d 1174, 1182 (D.C. Cir. 2004) (court has "inherent authority to review
26 classified material *ex parte, in camera* as part of its judicial review function") (citing cases), *cert.*
27

1 denied, 543 U.S. 1146 (2005); *Patterson v. Fed. Bureau of Investigation*, 893 F.2d 595, 600 n.9,
2 604-05 (3d Cir. 1990) (noting that “notwithstanding this imbalance between the parties, the D.C.
3 Circuit, as well as other circuits, have allowed the use of *in camera* affidavits in national security
4 cases”); *see also Holy Land Found. for Relief & Dev. v. Ashcroft*, 333 F.3d 156, 164 (D.C. Cir.
5 2003) (rejecting plaintiff’s “claim that the use of classified information disclosed only to the
6 court *ex parte* and *in camera* in the designation of a foreign terrorist organization . . . was
7 violative of due process”), *cert. denied*, 540 U.S. 1218 (2004); *People’s Mojahedin Org. of Iran*
8 *v. Dept. of State*, 327 F.3d 1238, 1242 (D.C. Cir. 2003) (same); *Global Relief Found. v. O’Neill*,
9 315 F.3d 748, 754 (7th Cir. 2002) (rejecting constitutional challenge to federal statute which
10 authorizes the district court’s *ex parte* and *in camera* consideration of classified evidence in
11 connection with a judicial challenge to an Executive decision to freeze the assets of entity that
12 assisted or sponsored terrorism), *cert. denied*, 540 U.S. 1003 (2003); *Torbet v. United Airlines*,
13 298 F.3d 1087, 1089 (9th Cir. 2002) (affirming district court’s dismissal of complaint
14 challenging airline search based, in part, on *in camera* review of sensitive security information);
15 *Doe v. Browner*, 902 F. Supp. 1240, 1250 n.7 (D. Nev. 1995) (dismissing environmental
16 challenge as moot based on *in camera* inspection of classified documents), *aff’d in part and*
17 *dismissed in part sub nom., Kasza v. Browner*, 133 F.3d 1159 (9th Cir. 1988).

18 Similarly, in cases where, as here, the Government has asserted the state secrets privilege,
19 courts routinely examine classified information on an *in camera, ex parte* basis, and on the basis
20 of that examination, make determinations that affect or even dictate the outcome of a case. *See,*
21 *e.g., Sterling v. Tenet*, 416 F.3d 338, 342 (4th Cir. 2005) (upholding dismissal based on
22 determination, after reviewing *in camera* affidavits, that any attempt by plaintiffs to make out a
23 prima facie case at trial would entail the revelation of state secrets), *cert. denied*, 126 S. Ct. 1052
24 (2006); *accord Kasza v. Browner*, 133 F.3d 1159, 1170 (9th Cir. 1998); *Edmonds v. U.S. Dept. of*
25 *Justice*, 323 F. Supp. 2d 65, 74 (D.D.C. 2004), *aff’d*, 161 Fed. Appx. 6 (D.C. Cir.), *cert. denied*,

1 126 S. Ct. 734 (2005); *Salisbury v. United States*, 690 F.2d 966, 974-77 (D.C. Cir. 1982); *El*
2 *Masri v. Tenet*, Civil Action No. 05-1417 (E.D. Va.), Order, May 12, 2006, attached as Ex. A.¹

3 In cases such as this one, where the national security of the United States is implicated, it
4 is well established that the Executive Branch is best positioned to judge the potential effects of
5 disclosure of sensitive information on the nation's security. See *Dept. of Navy v. Egan*, 484 U.S.
6 518, 529 (1988) ("Predictive judgment [about whether someone might 'compromise sensitive
7 information'] must be made by those with the necessary expertise in protecting classified
8 information."); *Central Intelligence Agency v. Sims*, 471 U.S. 159, 170 (1985) ("Congress
9 intended to give the Director of Central Intelligence broad power to protect the secrecy and
10 integrity of the intelligence process. The reasons are too obvious to call for enlarged discussion;
11 without such protections the Agency would be virtually impotent."). Indeed, the Supreme Court
12 has repeatedly recognized that courts are ill-equipped as an institution to judge harm to national
13 security. See *Egan*, 484 U.S. at 529 ("The Court also has recognized 'the generally accepted
14 view that foreign policy was the province and responsibility of the Executive.'") (quoting *Haig*,
15 453 U.S. at 293-94)); see also *Sims*, 471 U.S. at 180 ("weigh[ing] the variety of subtle and
16 complex factors in determining whether disclosure of information may lead to an unacceptable
17 risk of compromising the [nation's] intelligence-gathering process" is a task best left to the
18 Executive Branch and not attempted by the judiciary).

19 Thus, where, as here, the Executive Branch, through the Director of National Intelligence
20 and the Director of the National Security Agency, has determined that the needs of national
21 security demands that certain information be reviewed only by the Court *in camera* and *ex parte*,
22 Plaintiffs' due process concerns must be viewed in light of that determination. The "strong
23

24
25 ¹ See also *American-Arab Anti-Discrim. Comm. v. Reno*, 70 F.3d 1045, 1070 (9th Cir.
26 1995) (explaining that the effect of a successful invocation of the state secrets privilege is that
27 "the evidence is unavailable, as though a witness had died" and that even when the privilege
operates "as a complete shield to the government and results in the dismissal of a plaintiff's suit,
the information is simply unavailable and may not be used by either side") (internal quotation
marks and citations omitted).

1 interest of the government [in protecting against the disclosure of classified information] clearly
2 affects the nature . . . of the due process which must be afforded petitioners.” *Nat’l Council of*
3 *Resistance of Iran v. Dept. of State*, 251 F.3d 192, 208-09 (D.C. Cir. 2001); *see also Gilbert v.*
4 *Homar*, 520 U.S. 924, 930 (1997) (“it is by now well established that due process, unlike some
5 legal rules, is not a technical conception with a fixed content unrelated to time, place and
6 circumstances”) (internal quotation marks and citation omitted); *Morrissey v. Brewer*, 408 U.S.
7 471, 481 (1972) (“due process is flexible and calls for such procedural protections as the
8 particular situation demands”). In this situation, as the Court of Appeals has plainly held, *ex*
9 *parte* consideration is proper and Plaintiffs’ interests “as a litigant are satisfied by the *ex parte/in*
10 *camera* decision of an impartial district judge.” *Meridian Int’l Logistics, Inc.*, 939 F.2d at 745;
11 *see also In re Sealed Case No. 98-3077*, 151 F.3d 1059, 1075 (D.C. Cir. 1998) (“We recognize
12 that appellants cannot make factual arguments about materials they have not seen and to that
13 degree they are hampered in presenting their case. The alternatives, however, are sacrificing the
14 secrecy of the [materials] or leaving the issue unresolved at this critical juncture.”) (quoting *In re*
15 *John Doe Corp.*, 675 F.2d 482, 490 (2d Cir. 1982)).

16 The consequences that sometimes must flow from the United States’ compelling need to
17 protect national security information was demonstrated earlier this month by the decision of the
18 United States District Court for the Eastern District of Virginia in *El-Masri v. Tenet*, Civil Action
19 No. 05-1417 (E.D. Va.), attached as Ex. A. In *El-Masri*, in response to Plaintiff’s Complaint
20 making constitutional tort allegations against former CIA Director George Tenet, other CIA
21 employees, and private individuals concerning an “extraordinary rendition” program, the United
22 States moved to intervene and filed a formal claim of the state secrets privilege, supported by
23 both an unclassified and a classified *ex parte* declaration from the Director of the CIA. The
24 United States also sought dismissal or summary judgment on the ground that maintenance of the
25 suit would invariably lead to disclosure of its state secrets.

1 In its May 12, 2006, opinion, the District Court agreed. Finding that courts must “bear in
2 mind the Executive Branch’s preeminent authority over military and diplomatic matters and its
3 greater expertise relative to the judicial branch in predicting the effect of a particular disclosure
4 on national security,” Slip Op. at 9, the Court concluded that “there is no doubt that the state
5 secrets privilege is validly asserted here.” *Id.* at 10. Specifically, the Court found that Plaintiff’s
6 “publicly available complaint alleges a clandestine intelligence program, and the means and
7 methods the foreign intelligence services of this and other countries used to carry out the
8 program” and that “any admission or denial of these allegations . . . would reveal the means and
9 methods employed pursuant to this clandestine program and . . . would present a grave risk to
10 national security.” *Id.* Moreover, the Court found that state secrets in the form of details about
11 the classified rendition program were the “very subject of litigation,” *see id.* at 12-13, and
12 concluded that dismissal of Plaintiffs’ claims was the only appropriate disposition: “while
13 dismissal of the complaint deprives El-Masri of an American judicial forum for vindicating his
14 claims, well-established and controlling legal principles require that . . . El-Masri’s private
15 interests must give way to the national interests in preserving state secrets.” *Id.* at 14.

16 For the same reasons, dismissal is also the appropriate disposition of this case, and none
17 of the authority cited by Plaintiffs demands a different result. The cases upon which Plaintiffs
18 rely do not involve the *ex parte* submission of classified information. *Lynn v. Regents of Univ. of*
19 *Calif.*, 656 F.2d 1337 (9th Cir. 1981), involved a claim of gender discrimination brought by an
20 assistant professor who alleged she was denied merit salary increases and tenure. The Ninth
21 Circuit held that the district court’s *in camera, ex parte* review of the plaintiff’s tenure file
22 violated the plaintiff’s due process. *Id.* at 1345-46. And, in *Guenther II*, an appeal by taxpayers
23 of the Internal Revenue Commissioner’s finding of deficiency, the court found that the district
24 court’s review of an *ex parte* trial memorandum violated the plaintiffs’ due process. 939 F.2d
25 758. Indeed, the *Guenther* cases upon which Plaintiffs rely support the Government’s position
26 that classified information is properly considered by the Court *in camera* and *ex parte*. *See, e.g.,*

1 *Guenther I*, 889 F.2d at 884 (“And recently, we made clear that absent some ‘compelling
2 justification,’ ex parte communications will not be tolerated.”); *Guenther II*, 939 F.2d at 760
3 (affirming “compelling justification” principle); see also *United States v. Thompson*, 827 F.2d
4 1254, 1259 (9th Cir. 1987) (“situations where the court acts with the benefit of only one side’s
5 presentation are uneasy compromises with some overriding necessity, such as the need to act
6 quickly or to keep sensitive information from the opposing party”). Other cases in this circuit
7 further demonstrate the lack of merit to Plaintiffs’ position. See *United States v. Klimavicius-*
8 *Viloria*, 144 F.3d 1249, 1261 (9th Cir. 1998) (“In a case involving classified documents, . . . ex
9 parte, in camera hearings in which government counsel participates to the exclusion of defense
10 counsel are part of the process that the district court may use in order to decide the relevancy of
11 the information.”); *Kasza*, 133 F.3d at 1165 (affirming dismissal where district court “properly
12 considered classified declarations and documents in camera” in ruling on government’s
13 invocation of the state secrets privilege).

14 In sum, the Court has the inherent authority to consider classified information *in camera*
15 and *ex parte* without violating Plaintiffs’ right to due process and, thus, before proceeding with
16 the litigation of Plaintiffs’ claims on the merits, the Court should consider the materials
17 submitted by the United States in support of its assertion of the state secrets privilege in order to
18 fully understand and avoid the dangers that would result from any such litigation.

19 **II. PLAINTIFFS ARE NOT ENTITLED TO ACCESS TO THE CLASSIFIED**
20 **MATERIALS SUBMITTED *IN CAMERA*, *EX PARTE*.**

21 Plaintiffs claim that the Foreign Intelligence Surveillance Act (“FISA”), 50 U.S.C. § 1801
22 *et seq.*, creates a statutory mechanism that allows them access to the classified material that
23 forms the basis of the Government’s assertion of the state secrets privilege. In particular, they
24 rely on section 1806(f) of the FISA, which provides a basis for “an aggrieved person” to seek
25 judicial review of the legality of the FISA electronic surveillance. They claim that if the Court
26 intends to review the Government’s classified material, it should also provide Plaintiffs with
27

1 access to that material under the review procedures set forth in section 1806(f).² Plaintiffs,
2 however, are not entitled to review classified material under the FISA or any other mechanism.

3 It is well-established that, under the separation of powers established by the Constitution,
4 the Executive is exclusively responsible for the protection and control of national security
5 information, and the decision to grant or deny access to such information rests exclusively within
6 the discretion of the Executive. *See Egan*, 484 U.S. at 527-28 (noting that the Executive
7 supremacy on such decisions arises from President's role as Commander in Chief under Art. II,
8 § 2 of Constitution); *Dorfmont v. Brown*, 913 F.2d 1399, 1401 (9th Cir. 1990) ("a clearance may
9 be granted or retained only if 'clearly consistent with the interests of the national security'; "the
10 decision to grant or revoke a security clearance is committed to the discretion of the President by
11 law") (quoting *Egan*, 484 U.S. at 527).

12 As a corollary to this principle, a federal district court may not order the Executive to
13 grant opposing counsel or any other person access to classified information, and in keeping with
14 this rule, the Ninth Circuit and other courts repeatedly have rejected demands that opposing
15 counsel or parties be permitted access to classified material presented to the court *in camera* and
16 *ex parte*. *See Pollard*, 705 F.2d at 1153 (rejecting plaintiff's claim that counsel should have been
17 allowed access to materials reviewed *in camera* "where the claimed [FOIA] exemption involved
18

19 ² The following is the pertinent language of section 1806(f), on which Plaintiffs rely:

20 [W]henever a motion or request is made by an aggrieved person . . . to discover or
21 obtain applications or orders or other materials relating to electronic
22 surveillance . . . the United States district court . . . shall, notwithstanding any
23 other law, if the Attorney General files an affidavit under oath that disclosure or
24 an adversary hearing would harm the national security of the United States, review
25 *in camera* and *ex parte* the application, order, and such other materials relating to
26 the surveillance as may be necessary to determine whether the surveillance of the
aggrieved person was lawfully authorized and conducted. In making this
determination, the court may disclose to the aggrieved person, under appropriate
security procedures and protective orders, portions of the application, order, or
other materials relating to the surveillance only where such disclosure is necessary
to make an accurate determination of the legality of the surveillance.

27 50 U.S.C. § 1806(f). Plaintiffs also rely on a similar provision in 50 U.S.C. § 1845(f).

1 is the national defense or foreign policy secrecy exemption”); *see also People's Mojahedin Org.*
2 *of Iran*, 327 F.3d at 1242-43; *In re United States*, 1 F.3d 1251, WL 262658, *6 (Fed. Cir. 1993)
3 (fact that certain of the defense contractor plaintiff's employees already had access to the
4 classified material “does not divest the [Air Force Secretary] of his exclusive authority to control
5 access to other persons or limit his right to assert the privilege to prevent any disclosure in a
6 pending lawsuit”); *Salisbury v. United States*, 690 F.2d 966, 973-74 & n.3 (D.C. Cir. 1982) (“It is
7 well settled that a trial judge called upon to assess the legitimacy of a state secrets privilege claim
8 should not permit the requester's counsel to participate in an in camera examination of putatively
9 privileged material”); *Weberman v. Nat'l Security Agency*, 668 F.2d 676, 678 (2d Cir. 1982)
10 (“The risk presented by participation of counsel . . . outweighs the utility of counsel, or adversary
11 process Given these circumstances, [the district judge] was correct in . . . excluding counsel
12 from the in camera viewing”); *Hayden v. Nat'l Security Agency*, 608 F.2d 1381, 1385-86 (D.C.
13 Cir. 1979) (“it is not appropriate, and not possible without grave risk, to allow access to
14 classified defense-related material to counsel who lack security clearance”); *El-Masri*, Slip Op. at
15 13-14 (finding that clearing counsel for access to classified information is “plainly ineffective
16 where, as here, the entire aim of the suit is to prove the existence of state secrets”).

17 Thus, Plaintiffs' suggestion that the Court can establish “safeguards” for Plaintiffs to
18 review the classified material subject to the Government's assertion of the state secrets privilege
19 is incorrect. *See* Pltfs' Br. at 4. Indeed, Plaintiffs fail to cite a single case in support of their
20 assertion.³ Such “safeguards” merely present the opportunity for further disclosure of classified
21

22 ³ Plaintiffs' reliance on *DTM Research, L.L.C. v. AT&T Corp.*, 245 F.3d 327, 334 (4th
23 Cir. 2001), for their claim that this Court may grant them access to the relevant classified
24 information is misplaced. In that case, the Fourth Circuit upheld the Government's assertion of
25 the state secrets privilege and excluded the use of any of the material covered by the privilege,
26 but further determined that the exclusion of that material did not necessitate dismissal. *Id.* In
27 making this determination, the court did not grant the Plaintiffs access to the classified material,
as Plaintiffs request here. Moreover, as explained in the Government's assertion of the state
secrets privilege, state secrets are so central to the allegations in Plaintiffs' Amended Complaint
that any attempt to proceed will threaten disclosure of the privileged matters. *See* U.S. Mem. at
14-29.

1 information. *See, e.g., Sterling v. Tenet*, 416 F.3d 338, 348 (4th Cir. 2005), *cert. denied*, 126 S.
2 Ct. 1052 (2006) (“Such procedures, whatever they might be, still entail considerable risk. . . . At
3 best, special accommodations give rise to added opportunity for leaked information. At worst,
4 that information would become public, placing covert agents and intelligence sources alike at
5 grave personal risk.”); *Halkin v. Helms*, 598 F.2d 1, 7 (D.C. Cir. 1978) (“*Halkin P*”) (“However
6 helpful to the court the informed advocacy of the Plaintiffs’ counsel may be, we must be
7 especially careful not to order any dissemination of information asserted to be privileged state
8 secrets”; “[p]rotective orders cannot prevent inadvertent disclosure nor reduce the damage to
9 national security of the nation which may result.”).

10 Plaintiffs attempt to avoid the well-established rule that their counsel do not get access to
11 classified material by relying on the judicial review mechanism set forth in section 1806(f) of the
12 FISA. Their reliance on FISA, however, is mistaken. Significantly, Plaintiffs’ claims are based
13 on their contention that the alleged surveillance activities should have occurred under FISA, but
14 allegedly did not, *see, e.g., Am. Compl.* ¶¶ 90-99, whereas the review available under section
15 1806(f) is available only when electronic surveillance did, in fact, occur “under this chapter.” 50
16 U.S.C. § 1806(f); *see id.* (authorizes court to review *in camera* and *ex parte* “the application,
17 order and such other materials relating to the surveillance. . . .”). Thus, by their own allegations,
18 section 1806(f) is inapplicable to Plaintiffs.

19 In any event, even if Plaintiffs claim that alleged surveillance occurred under the FISA,
20 only “an aggrieved person” can utilize the statutory mechanism for seeking judicial review of the
21 legality of FISA surveillance.⁴ *See* 50 U.S.C. § 1806(f). But Plaintiffs cannot demonstrate that
22 they are aggrieved persons under the FISA because the Government’s privilege assertion covers
23 any information tending to confirm or deny (a) the alleged intelligence activities, (b) whether
24 AT&T was involved with any such activity, and (c) whether a particular individual’s

25
26 ⁴ FISA defines an “aggrieved person” as “a person who is the target of an electronic
27 surveillance or any other person whose communications or activities were subject to electronic
28 surveillance.” 50 U.S.C. § 1801(k).

1 communications were intercepted as a result of any such activity. *See* U.S. Mem. at 17-18.
2 Thus, because Plaintiffs lack the information necessary for them to demonstrate that they are
3 aggrieved persons under the FISA, they lack standing to invoke that statute's judicial review
4 provisions. *See Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560-61 (1992). Moreover, in order
5 to initiate judicial review under section 1806(f), Plaintiffs would have to show that electronic
6 surveillance as defined by FISA, 50 U.S.C. § 1801(f), actually occurred. The Government's
7 assertion of the state secrets privilege precludes any such showing as well.

8 Finally, even if section 1806(f) was applicable to Plaintiffs' allegations and arguably
9 could be interpreted to require disclosure of information to uncleared counsel,⁵ it should not be
10 interpreted in that manner because doing so would be inconsistent with the President's powers to
11 control access to classified information and with the power to assert the state secrets privilege.⁶
12 *See Nadarajah v. Gonzales*, 443 F.3d 1069,1076 (9th Cir. 2006) (“[I]f an otherwise acceptable
13

14 ⁵ Plaintiffs are incorrect that FISA allows them immediate access to the classified
15 material submitted to the Court. Rather, the FISA review process requires the Court first to
16 review (upon an assertion of privilege by the Attorney General) the relevant material *in camera*,
17 *ex parte* “as may be necessary to determine whether the surveillance of the aggrieved person was
18 lawfully authorized and conducted.” 50 U.S.C. § 1806(f). The FISA allows very limited
19 disclosure of the relevant FISA material only where the Court – after conducting this *in camera*,
20 *ex parte* review – determines that “such disclosure is necessary to make an accurate
21 determination of the legality of the surveillance.” *Id.* Indeed, since the enactment of FISA, every
22 court to review the legality of a FISA electronic surveillance or physical search pursuant to *in camera*,
23 *ex parte* review has upheld the Government's actions, and no court has disclosed the
24 underlying materials to the moving party. *See, e.g., United States v. Hamide*, 914 F.2d 1147 (9th
25 Cir. 1990); *United States v. Squillacote*, 221 F.3d 542 (4th Cir. 2000); *United States v. Johnson*,
26 952 F.2d 565 (1st Cir. 1991); *United States v. Isa*, 923 F.2d 1300 (8th Cir. 1991); *United States*
27 *v. Badia*, 827 F.2d 1458 (11th Cir. 1987); *United States v. Ott*, 827 F.2d 473 (9th Cir. 1987);
28 *United States v. Duggan*, 743 F.2d 59 (2d Cir. 1984); *United States v. Belfield*, 692 F.2d 141
(D.C. Cir. 1982).

23 ⁶ Such an interpretation would also be inconsistent with, and could not override, the
24 statutory privilege that the United States has asserted concerning the activities and information of
25 the NSA. *See* Declaration of Keith B. Alexander, Director of the National Security Agency, U.S.
26 Mem., Attachment 2, ¶ 6 (quoting section 6 of the National Security Agency Act of 1959, Public
27 Law No. 86-36, codified as a note to 50 U.S.C. § 402: “[n]othing in this Act or any other law . . .
28 shall be construed to require the disclosure of the organization or any function of the National
Security Agency [or] any information with respect to the activities thereof. . . .”) (emphasis
added); *see also* Declaration of John D. Negroponte, Director of National Intelligence, U.S.
Mem., Attachment 1 (quoting 50 U.S.C. § 403-1(i)(1): “The Director of National Intelligence
shall protect intelligence sources and methods from disclosure”).

1 construction of a statute would raise serious constitutional problems, and where an alternative
2 interpretation of the statute is ‘fairly possible,’ we are obligated to construe the statute to avoid
3 such problems.”) (quoting *INS v. St. Cyr*, 533 U.S. 289, 299-300 (2001)) (citation omitted). In
4 addition, when Congress intentionally seeks to restrict or regulate presidential action through
5 legislation, it must make that intention clear. See *Armstrong v. Bush*, 924 F.2d 282, 289 (D.C.
6 Cir. 1991) (“[l]egislation regulating presidential action . . . raises ‘serious’ practical, political,
7 and constitutional questions that warrant careful congressional and presidential consideration”)
8 (citing *United States v. Bass*, 404 U.S. 336, 350 (1971)). Section 1806(f) does not set forth a
9 clear intention to restrict the President’s constitutionally-imposed authority to protect and control
10 national security information in the context of this case. See *Egan*, 484 U.S. at 527.

11 **III. PLAINTIFFS HAVE OFFERED NO VALID REASON FOR THE COURT TO**
12 **FOREGO REVIEW OF THE *IN CAMERA*, *EX PARTE* MATERIALS.**

13 Plaintiffs’ remaining arguments – that the Court need not review the *in camera*, *ex parte*
14 materials because Plaintiffs can prove their *prima facie* case based on the public record, see Pltfs’
15 Br. at 5-9, that the Court’s review of the *in camera*, *ex parte* materials is premature, see *id.* at 10-
16 14, and that it would be appropriate to permit discovery into any certifications AT&T may have
17 received from the United States, see *id.* at 14 – all reflect a fundamental misconception of the
18 scope, nature and effect of the Government’s invocation of the state secrets privilege.

19 Although the primary reasons for rejecting Plaintiffs’ arguments are set forth in the
20 Government’s *in camera*, *ex parte* materials, several arguments that can be made on the public
21 record demonstrate that Plaintiffs’ position is without merit. Plaintiffs’ primary argument for
22 deferring review of the *in camera*, *ex parte* materials is that they “can sustain their *prima facie*
23 case without resort to the classified materials.” Pltfs’ Br. at 5. But this argument ignores the
24 well-established rule that if “the ‘very subject matter of the action’ is a state secret, then the court
25 should dismiss the plaintiff’s action based solely on the invocation of the state secrets privilege.”
26 *Kasza*, 133 F.3d at 1166 (citing *United States v. Reynolds*, 345 U.S. 1, 11 n.26 (1953)); see also

1 *Totten v. United States*, 92 U.S. 105, 107 (1875) (“[P]ublic policy forbids the maintenance of any
2 suit in a court of justice, the trial of which would inevitably lead to the disclosure of matters
3 which the law itself regards as confidential, and respecting which it will not allow the confidence
4 to be violated.”); *see also Tenet v. Doe*, 544 U.S. 1, 8 (2005) (applying *Totten* to bar a suit
5 brought by former Soviet double agents seeking to enforce their alleged employment agreements
6 with the CIA and making clear that the *Totten* bar applies whenever a party’s “success depends
7 upon the existence of [a] secret espionage relationship with the government”). In such cases, the
8 state secrets are “so central to the subject matter of the litigation that any attempt to proceed will
9 threaten disclosure of the privileged matters.” *Fitzgerald v. Penthouse Int’l, Ltd.*, 776 F.2d 1236,
10 1241-42 (4th Cir. 1985). For the reasons discussed in the Government’s *in camera, ex parte*
11 filing, the very subject matter of Plaintiffs’ allegations is a state secret and further litigation
12 would inevitably risk their disclosure.

13 Even if the very subject matter of Plaintiffs’ allegations were not state secrets, Plaintiffs
14 are wrong to claim that they can make out a *prima facie* claim absent the excluded state secrets.
15 As noted above, in order to prevail on any of their claims, Plaintiffs bear the burden of
16 establishing standing and must, at an “irreducible constitutional minimum,” demonstrate (1) an
17 injury-in-fact, (2) a causal connection between the injury and the conduct complained of, and (3)
18 a likelihood that the injury will be redressed by a favorable decision. *Lujan*, 504 U.S. at 560-61.
19 In meeting that burden, the named Plaintiffs must demonstrate an actual or imminent – not
20 speculative or hypothetical – injury that is particularized as to them; they cannot rely on alleged
21 injuries to unnamed members of a purported class. And to obtain prospective relief, Plaintiffs
22 must show that they are “immediately in danger of sustaining some direct injury” as the result of
23 the challenged conduct. *City of Los Angeles v. Lyons*, 461 U.S. 95, 102 (1983); *O’Shea v.*
24 *Littleton*, 414 U.S. 488, 495-96 (1974).

25 As demonstrated in the Government’s public briefs and declarations, Plaintiffs cannot
26 prove these jurisdictional elements without information covered by the state secrets assertion.

1 The Government’s privilege assertion covers any information that tends to confirm or deny (a)
 2 the alleged intelligence activities, (b) whether AT&T was involved with any such activity, and
 3 (c) whether a particular individual’s communications were intercepted as a result of any such
 4 activity. See Declaration of John D. Negroponte, Director of National Intelligence, U.S. Mem.,
 5 Attachment 1 (“Negroponte Decl.”), ¶¶ 11-12. Without these facts – which must be removed
 6 from the case as a result of the state secrets assertion – Plaintiffs cannot establish any alleged
 7 injury that is fairly traceable to AT&T.⁷ Thus, regardless of whether they adequately allege such
 8 facts, Plaintiffs ultimately will not be able to prove injury-in-fact or causation—and thus cannot
 9 establish this Court’s jurisdiction, let alone sustain a *prima facie* case, without information
 10 subject to the state secrets privilege.⁸

11

12 ⁷ Because jurisdictional issues must be examined as a threshold question, *see, e.g., Steel*
 13 *Co. v. Citizens for a Better Environment*, 523 U.S. 83, 94-95 (1998), if the Court were to
 14 determine on the basis of the public record that Plaintiffs failed to establish their standing
 15 because, for example, Plaintiffs have failed to meet their burden to do so as a matter of law, or
 16 because it is clear from the public record that, in light of United States’ inability to confirm or
 17 deny whether any individual Plaintiff is the subject of surveillance, the Court may find it
 unnecessary to review the United States’ *in camera, ex parte* submissions, and may dismiss this
 case on that ground alone. Otherwise, however, review of the materials submitted *in camera* and
ex parte is necessary to adjudicate the state secrets issues posed by this case. As a result, the
 Court could dismiss this case on the basis of the Government’s public assertion of the state
 secrets privilege.

18 ⁸ As the United States noted in its public brief, to the extent Plaintiffs challenge the
 19 Terrorist Surveillance Program (“TSP”), *see, e.g., Am. Compl.* 32-37, the allegations in the
 20 Complaint are insufficient on their face to establish standing even apart from the state secrets
 21 issue because Plaintiffs fail to demonstrate that they fall anywhere near the scope of that
 22 program. Plaintiffs do not claim to be, or to communicate with, members or affiliates of al
 Qaeda – indeed, Plaintiffs expressly *exclude* from their purported class any foreign powers or
 23 agents of foreign powers, “including without limitation anyone who knowingly engages in
 24 sabotage or international terrorism, or activities that are in preparation therefore.” *Am. Compl.*
 ¶ 70. The named Plaintiffs thus are in no different position from any other citizen or AT&T
 25 subscriber who falls *outside* the narrow scope of the TSP but nonetheless disagrees with the
 26 program. Such a generalized grievance is clearly insufficient to support either constitutional or
 27 prudential standing to challenge the TSP. *See Halkin v. Helms*, 690 F.2d 977, 1001-03 (D.C. Cir.
 1982) (“*Halkin II*”) (holding that individuals and organizations opposed to the Vietnam War
 lacked standing to challenge intelligence activities because they did not adequately allege that
 they were (or immediately would be) subject to such activities; thus, their claims were “nothing
 more than a generalized grievance against the intelligence-gathering methods sanctioned by the
 President”) (internal quotation marks and citation omitted); *United Presbyterian Church in the*
U.S.A. v. Reagan, 738 F.2d 1375, 1380 (D.C. Cir. 1984) (rejecting generalized challenge to
 alleged unlawful surveillance). To the extent Plaintiffs allege classified intelligence activities

1 Plaintiffs' inability to sustain a *prima facie* case is not limited to their inability to prove
2 their standing. More generally, as the Government explained in its public brief, adjudicating
3 each claim in the Amended Complaint would require confirmation or denial of the existence,
4 scope, and potential targets of alleged intelligence activities, as well as AT&T's alleged
5 involvement in such activities.⁹ Because such information cannot be confirmed or denied
6 without causing exceptionally grave damage to the national security, Plaintiffs' attempt to make
7 out a *prima facie* case would run into privileged information. Where, as here, a plaintiff cannot
8 make out a *prima facie* case in support of its claims absent the excluded state secrets, the case
9 must be dismissed. *See Kasza*, 133 F.3d at 1166; *Halkin II*, 690 F.2d at 998-99; *Fitzgerald*, 776
10 F.2d at 1240-41.

11 Plaintiffs' argument also fails to recognize that litigation is not limited to determining
12 whether a plaintiff can establish a *prima facie* case. For that very reason, courts have recognized
13 that if the state secrets privilege "deprives the *defendant* of information that would otherwise
14 give the defendant a valid defense to the claim, then the court may grant summary judgment to
15 the defendant." *Kasza*, 133 F.3d at 1166 (quoting *Bareford v. General Dynamics Corp.*, 973
16 F.2d 1138, 1141 (5th Cir. 1992)); *see also Molerio v. Fed. Bureau of Investigation*, 749 F.2d
17 815, 825 (D.C. Cir. 1984) (granting summary judgment where state secrets privilege precluded
18 _____
19 beyond the TSP, Plaintiffs could not prove such allegations in light of the state secrets assertion.

20 ⁹ As the United States demonstrated in its public brief, to prove their FISA claim (as
21 alleged in Count I), Plaintiffs would have to show that AT&T intentionally acquired, under color
22 of law and by means of a surveillance device within the United States, the contents of one or
23 more wire communications to or from Plaintiffs. *See* Am Compl. ¶¶ 93-94; 50 U.S.C.
24 §§ 1801(f), 1809, 1810. Likewise, to prove their claim under 18 U.S.C. § 2511 (as alleged in
25 Count III), Plaintiffs would have to demonstrate that AT&T intentionally intercepted, disclosed,
26 used, and/or divulged the contents of Plaintiffs' wire or electronic communications. *See* Am.
27 Compl. ¶¶ 102-07. Plaintiffs' claims under 47 U.S.C. § 605, 18 U.S.C. § 2702, and Cal. Bus. &
28 Prof. Code §§ 17200, *et seq.*, all require similar proof: the acquisition and/or disclosure of
Plaintiffs' communications and related information. And Plaintiffs must also prove, for each of
their statutory claims, that any alleged interception or disclosure was not authorized by the
Government. Despite Plaintiffs' unsupported assumption that they could demonstrate some or
all of these necessary facts on the basis of the public record, the Government's submissions make
clear that any information tending to confirm or deny the alleged activities, or any alleged AT&T
involvement, is subject to the state secrets privilege. *See* Negroponde Decl. ¶¶ 11-12.

1 the Government from using a valid defense). In this case – as noted in the United States’ public
2 brief and as demonstrated in the *in camera, ex parte* materials – neither AT&T nor the
3 Government could defend this action on the grounds that, among other things, the activities
4 alleged by the Complaint (i) were authorized by the Government; (ii) did not require a warrant
5 under the Fourth Amendment; (iii) were reasonable under the Fourth Amendment; or (iv) were
6 otherwise authorized by law. *See* U.S. Mem. at 14-29.

7 Plaintiffs suggest that the Court could adjudicate whether AT&T received any
8 certification or authorization from the Government relating to the alleged surveillance activity.
9 They are mistaken. The United States has explained that the state secrets assertion “covers any
10 information tending to confirm or deny” whether “AT&T was involved with any” of the “alleged
11 intelligence activities.” *See* U.S. Mem. at 17-18. Clearly, the existence or non-existence of any
12 certification or authorization by the Government relating to any AT&T activity would be
13 information tending to confirm or deny AT&T’s involvement in any alleged intelligence activity.
14 Thus, any such activity would fall within the Government’s state secrets assertion, and the Court
15 could not adjudicate, or allow discovery regarding, whether any Government certification or
16 authorization exists without considering the Government’s assertion of the state secrets privilege.
17 *See id.* at 23.¹⁰

18 Finally, Plaintiffs argue that before the Court can review the *in camera, ex parte*
19 materials, the Government must make a more specific – *i.e.*, public – showing about the
20 information subject to the state secrets privilege. But requiring such a showing would be
21 improper where, as here, it would “force ‘disclosure of the very thing the privilege is designed to
22 protect.’” *Ellsberg v. Mitchell*, 709 F.2d 51, 63 (D.C. Cir. 1983) (quoting *United States v.*
23 *Reynolds*, 345 U.S. 1, 8 (1953)); *see also* 709 F.2d at 63 (noting the Court’s “[f]ear” that “an
24

25 ¹⁰ Plaintiffs argue that 47 U.S.C. § 2511(2)(a)(ii) actually requires discovery of any
26 certifications. That is simply wrong. That provision precludes any entity that has received such
27 a certification from disclosing that certification “except as may otherwise be required by legal
28 process.” *Id.* Moreover, any “legal process” includes the determination of whether any privilege,
including the state secrets privilege or any statutory privilege, prohibits such disclosure.

1 insufficient public justification result in denial of the privilege entirely might induce the
2 government's representatives to reveal some material that, in the interest of national security,
3 ought not to be uncovered"; further noting the "considerable variety in the situations in which a
4 state secrets privilege may be fairly asserted"). As DNI Negroponete states in his Public
5 Declaration, "any further elaboration on the public record concerning these matters [covered by
6 his Declaration] would reveal information that could cause the very harms my assertion of the
7 state secrets privilege is intended to prevent." See Negroponete Decl. ¶¶ 11-12. In light of this
8 determination by the nation's highest-ranking intelligence official, the Government cannot say
9 more publicly, and should not – and cannot – be penalized in this litigation because it has done
10 nothing other than take the steps necessary to protect the national security of the United States.¹¹

11 Not surprisingly, Plaintiffs are unable to point to any state secrets case in which the court
12 has refused to review *in camera*, *ex parte* materials on the ground that the Government had
13 insufficiently described the state secrets on the public record. Instead, *Nixon v. Sirica*, 487 F.2d
14 700 (D.C. Cir. 1973) (*en banc*), on which Plaintiffs rely for the proposition that a more
15 particularized public showing must be made before a court conducts an *in camera* review of
16 privileged materials, is a case that involving the assertion of *executive privilege*, not the state
17 secrets privilege.¹² *Id.* at 715-16.

18
19 ¹¹ See, e.g., *In re United States*, 872 F.2d 472, 476 (D.C. Cir. 1989) ("Notions of
20 sovereign immunity preclude any further adverse consequence to the government, such as
21 alteration of procedural or substantive rules."); *Salisbury*, 690 F.2d at 975 ("when the
22 government is defendant . . . an adverse finding cannot be rendered against it as the price of
asserting an evidentiary privilege"); *Halkin I*, 598 F.2d at 10 (rejecting as "faulty" the premise
"that the defendants should not be permitted to avoid liability for unconstitutional acts by
asserting a privilege which would prevent plaintiffs from proving their case").

23 ¹² The executive privilege, like the state secrets privilege, is constitutionally grounded.
24 The executive privilege, however, protects the President's generalized interest in the
25 confidentiality of his communications, and, as *Nixon* establishes, is a qualified privilege (at least
26 in criminal cases). See 487 F.2d at 716. The state secrets privilege, on the other hand, is a
27 privilege that directly derives from the President's constitutional responsibility to determine,
based on his particular expertise, which disclosures will result in harm to the national security.
Once properly invoked, the state secrets privilege is absolute. *In re Under Seal*, 945 F.2d 1285,
1288 (4th Cir. 1991); see also *Halkin II*, 690 F.2d at 980 ("[S]ecrets of state – matters the
revelation of which reasonably could be seen as a threat to the military or diplomatic interest of

1 Instead, Plaintiffs try to contrast the Government’s public filings in this case with the
2 materials filed on the public record in *Kasza v. Browner*, 133 F.3d 1159 (9th Cir. 1998).
3 Although there is no indication in *Kasza* (and no basis in law or logic) to suggest that the Court
4 was creating a minimum requirement for public descriptions of state secrets assertions, in this
5 case the Government has made a similar public showing to that made in *Kasza*. In *Kasza*, the
6 declarant identified categories of information that were validly classified, describing those
7 categories in general terms, such as, for example, “program names”; “missions”; “capabilities”;
8 “intelligence sources and methods”; “security sensitive environmental data”; and “military plans,
9 weapons or operations.” *Id.* at 1168-69; *see also Edmonds*, 323 F. Supp. 2d at 74 (upholding
10 assertion of state secrets privilege and granting defendant’s motion to dismiss where the Attorney
11 General concluded that “further disclosure of the information underlying this case, including the
12 nature of the duties of plaintiff or the other contract translators at issue in this case reasonably
13 could be expected to cause serious damage to the national security interests of the United States”
14 and finding this assertion “similar to the one submitted to the court in *Kasza*”).

15 The United States’ public filings in this case are no less specific than the public
16 submissions made in *Kasza* and *Edmonds*. For example, DNI Negroponte states in his Public
17 Declaration that to disclose additional details regarding the Terrorist Surveillance Program
18 beyond the facts already disclosed by the President would disclose “classified intelligence
19 information” and reveal “intelligence sources and methods,” as a result of which adversaries of
20 the United States would be able “to avoid detection by the U.S. Intelligence Community and/or
21 take measures to defeat or neutralize U.S. intelligence collection, posing a serious threat of
22 damage to the United States’ national security interests.” Negroponte Decl. ¶ 11; *see also El-*
23 *Masri*, Slip Op. at 10-11 (finding that even where Government had made “a general admission
24 that rendition exists,” the Government “validly claimed as state secrets” the “operational details
25 of the extraordinary rendition program”). With respect to Plaintiffs’ allegations regarding other

26 _____
27 the nation – are absolutely privileged from disclosure in the courts.”).

1 purported activities of the NSA, including allegations about NSA's purported involvement with
2 AT&T, DNI Negroponte further states that the United States can neither confirm nor deny
3 allegations concerning "intelligence activities," "sources," "methods," "relationships," or
4 "targets." Negroponte Decl. ¶ 12. And DNI Negroponte goes on to note that "disclosure of those
5 who are targeted by such activities would compromise the collection of intelligence information
6 just as disclosure of those who do are not targeted would reveal to adversaries that certain
7 communications channels are secure or, more broadly, would tend to reveal the methods being
8 used to conduct surveillance." *Id.*

9 In sum, where (as here) requiring further public descriptions of the state secrets assertion
10 would "force 'disclosure of the very thing the privilege is designed to protect,'" *Ellsberg*, 709
11 F.2d at 63 (citing *Reynolds*, 345 U.S. at 8), and where (as here) the Government has made a
12 public showing similar to that in *Kasza*, 133 F.3d at 1168-69, there is no reason for the Court to
13 require further public disclosures before reviewing the *in camera*, *ex parte* materials.

14 CONCLUSION

15 For the reasons stated herein, the Court should consider the United States' *in camera*, *ex*
16 *parte* submissions and rule on the Government's assertion of the state secrets privilege and its
17 Motion to Dismiss or, in the Alternative, for Summary Judgment before taking any further action
18 in this case.

19 Respectfully submitted,

20 PETER D. KEISLER
Assistant Attorney General, Civil Division

21 CARL J. NICHOLS
Deputy Assistant Attorney General

22 DOUGLAS N. LETTER
Terrorism Litigation Counsel

23 JOSEPH H. HUNT
Director, Federal Programs Branch

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

ANTHONY J. COPPOLINO
Special Litigation Counsel
tony.coppolino@usdoj.gov

s/ Renée S. Orleans
RENÉE S. ORLEANS
renee.orleans@usdoj.gov
ANDREW H. TANNENBAUM
andrew.tannenbaum@usdoj.gov
U.S. Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Avenue, NW
Washington, D.C. 20001
Phone: (202) 514-4782/(202) 514-4263
Fax: (202) 616-8460/(202) 616-8202/(202) 318-2461

DATED: May 24, 2006

Attorneys for Intervenor Defendant United States

CERTIFICATE OF SERVICE

I hereby certify that the foregoing **UNITED STATES' RESPONSE TO PLAINTIFFS' MEMORANDUM OF POINTS AND AUTHORITIES IN RESPONSE TO THE COURT'S MAY 17, 2006 MINUTE ORDER** will be served by means of the Court's CM/ECF system, which will send notifications of such filing to the following:

Electronic Frontier Foundation
Cindy Cohn
Lee Tien
Kurt Opsahl
Kevin S. Bankston
Corynne McSherry
James S. Tyre
545 Shotwell Street
San Francisco, CA 94110

Lerach Coughlin Stoia Geller Rudman & Robbins LLP
Reed R. Kathrein
Jeff D. Friedman
Shana E. Scarlett
100 Pine Street, Suite 2600
San Francisco, CA 94111

Traber & Voorhees
Bert Voorhees
Theresa M. Traber
128 North Fair Oaks Avenue, Suite 204
Pasadena, CA 91103

Pillsbury Winthrop Shaw Pittman LLP
Bruce A. Ericson
David L. Anderson
Patrick S. Thompson
Jacob R. Sorensen
Brian J. Wong
50 Fremont Street
PO Box 7880
San Francisco, CA 94120-7880

Sidley & Austin LLP
David W. Carpenter
Bradford Berenson
Edward R. McNicholas
David L. Lawson
1501 K Street, NW
Washington, DC 20005

s/ Renée S. Orleans

EXHIBIT F

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

TASH HEPTING, GREGORY HICKS
CAROLYN JEWEL and ERIK KNUTZEN
on Behalf of Themselves and All Others
Similarly Situated,

Plaintiffs,

v.

AT&T CORP., AT&T INC. and
DOES 1-20, inclusive,

Defendants.

Case No. C-06-0672-VRW

**DECLARATION OF
JOHN D. NEGROPONTE,
DIRECTOR OF NATIONAL
INTELLIGENCE**

I, John D. Negroponte, declare as follows:

INTRODUCTION

1. I am the Director of National Intelligence (DNI) of the United States. I have held this position since April 21, 2005. From June 28, 2004, until appointed to be DNI, I served as United States Ambassador to Iraq. From September 18, 2001, until my appointment in Iraq, I served as the United States Permanent Representative to the United Nations. I have also served as Ambassador to Honduras (1981-1985), Mexico (1989-1993), the Philippines (1993-1996), and as Deputy Assistant to the President for National Security Affairs (1987-1989).

2. In the course of my official duties, I have been advised of this lawsuit and the allegations at issue in this case. The statements made herein are based on my personal knowledge, as well as on information provided to me in my official capacity as DNI, and on my personal evaluation of that information. In personally considering this matter, I have executed a separate classified declaration dated May 12, 2006, and filed *in camera* and *ex parte* in this case. Moreover, I have read and personally considered the information contained in the *In Camera, Ex Parte* Declaration of Lt. Gen. Keith B. Alexander filed in this case. General Alexander is the

DECLARATION OF JOHN D. NEGROPONTE,
DIRECTOR OF NATIONAL INTELLIGENCE
Case No. C 06-0672-JCS

1 Director of the National Security Agency ("NSA"), and is responsible for directing the NSA,
 2 overseeing the operations undertaken to carry out its mission, and by specific charge from the
 3 President and the DNI, protecting NSA activities and intelligence sources and methods.

4 3. The purpose of this declaration is to formally assert, in my capacity as DNI and
 5 head of the United States Intelligence Community, the military and state secrets privilege
 6 (hereafter "state secrets privilege"), as well as a statutory privilege under the National Security
 7 Act, *see* 50 U.S.C. § 403-1(i)(1), in order to protect intelligence information, sources and
 8 methods that are implicated by the allegations in this case. Disclosure of the information
 9 covered by these privilege assertions reasonably could be expected to cause exceptionally grave
 10 damage to the national security of the United States and, therefore, should be excluded from any
 11 use in this case. In addition, I concur with General Alexander's conclusion that the risk is great
 12 that further litigation will risk the disclosure of information harmful to the national security of
 13 the United States and, accordingly, this case should be dismissed. *See* Declaration of Lt. Gen.
 14 Keith B. Alexander, Director, National Security Agency.

15 **BACKGROUND ON DIRECTOR OF NATIONAL INTELLIGENCE**

16 4. The position of Director of National Intelligence was created by Congress in the
 17 Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, §§ 1011(a) and
 18 1097, 118 Stat. 3638, 3643-63, 3698-99 (2004) (amending sections 102 through 104 of the Title
 19 I of the National Security Act of 1947). Subject to the authority, direction, and control of the
 20 President, the DNI serves as the head of the U.S. Intelligence Community and as the principal
 21 advisor to the President, the National Security Council, and the Homeland Security Council, for
 22 intelligence-related matters related to national security. *See* 50 U.S.C. § 403(b)(1), (2).

23 5. The "United States Intelligence Community" includes the Office of the Director
 24 of National Intelligence; the Central Intelligence Agency; the National Security Agency; the
 25 Defense Intelligence Agency; the National Geospatial-Intelligence Agency; the National
 26 Reconnaissance Office; other offices within the Department of Defense for the collection of

1 specialized national intelligence through reconnaissance programs; the intelligence elements of
2 the military services, the Federal Bureau of Investigation, the Department of Treasury, the
3 Department of Energy, Drug Enforcement Administration, and the Coast Guard; the Bureau of
4 Intelligence and Research of the Department of State; the elements of the Department of
5 Homeland Security concerned with the analysis of intelligence information; and such other
6 elements of any other department or agency as may be designated by the President, or jointly
7 designated by the DNI and heads of the department or agency concerned, as an element of the
8 Intelligence Community. *See* 50 U.S.C. § 401a(4).

9 6. The responsibilities and authorities of the DNI are set forth in the National
10 Security Act, as amended. *See* 50 U.S.C. § 403-1. These responsibilities include ensuring that
11 national intelligence is provided to the President, the heads of the departments and agencies of
12 the Executive Branch, the Chairman of the Joint Chiefs of Staff and senior military commanders,
13 and the Senate and House of Representatives and committees thereof. 50 U.S.C. § 403-1(a)(1).
14 The DNI is also charged with establishing the objectives of, determining the requirements and
15 priorities for, and managing and directing the tasking, collection, analysis, production, and
16 dissemination of national intelligence by elements of the Intelligence Community. *Id.* § 403-
17 1(f)(1)(A)(i) and (ii). The DNI is also responsible for developing and determining, based on
18 proposals submitted by heads of agencies and departments within the Intelligence Community,
19 an annual consolidated budget for the National Intelligence Program for presentation to the
20 President, and for ensuring the effective execution of the annual budget for intelligence and
21 intelligence-related activities, and for managing and allotting appropriations for the National
22 Intelligence Program. *Id.* § 403-1(c)(1)-(5).

23 7. In addition, the National Security Act of 1947, as amended, provides that "The
24 Director of National Intelligence shall protect intelligence sources and methods from
25 unauthorized disclosure." 50 U.S.C. § 403-1(i)(1). Consistent with this responsibility, the DNI
26 establishes and implements guidelines for the Intelligence Community for the classification of

27 DECLARATION OF JOHN D. NEGROPONTE,
28 DIRECTOR OF NATIONAL INTELLIGENCE
Case No. C 06-0672-ICS

Case 3:06-cv-00672-VRW Document 124-2 Filed 05/13/2006 Page 4 of 7

1 information under applicable law, Executive Orders, or other Presidential directives and access
2 and dissemination of intelligence. *Id.* § 403-1(i)(2)(A), (B). In particular, the DNI is responsible
3 for the establishment of uniform standards and procedures for the grant of access to Sensitive
4 Compartmented Information ("SCI") to any officer or employee of any agency or department of
5 the United States, and for ensuring consistent implementation of those standards throughout such
6 departments and agencies. *Id.* § 403-1(j)(1), (2).

7 8. By virtue of my position as the DNI, and unless otherwise directed by the
8 President, I have access to all intelligence related to the national security that is collected by any
9 department, agency, or other entity of the United States. Pursuant to Executive Order No.
10 12958, 3 C.F.R. § 333 (1995), as amended by Executive Order 13292 (March 25, 2003),
11 reprinted as amended in 50 U.S.C.A. § 435 at 93 (Supp. 2004), the President has authorized me
12 to exercise original TOP SECRET classification authority. My classified declaration, as well as
13 the classified declaration of General Alexander on which I relied in this case, are properly
14 classified under § 1.3 of Executive Order 12958, as amended, because the public disclosure of
15 the information contained in those declarations could reasonably be expected to cause serious
16 damage to the foreign policy and national security of the United States.

17 **ASSERTION OF THE STATE SECRETS PRIVILEGE**

18 9. After careful and actual personal consideration of the matter, I have determined
19 that the disclosure of certain information implicated by Plaintiffs' claims—as set forth here and
20 described in more detail in my classified declaration and in the classified declaration of General
21 Alexander—could reasonably be expected to cause exceptionally grave damage to the national
22 security of the United States and, thus, must be protected from disclosure and excluded from this
23 case. Thus, as to this information, I formally invoke and assert the state secrets privilege. In
24 addition, it is my judgment that any attempt to proceed in the case will substantially risk the
25 disclosure of the privileged information described briefly herein, and in more detail in the
26 classified declarations, and will cause exceptionally grave damage to the national security of the

27 DECLARATION OF JOHN D. NEGROPONTE,
28 DIRECTOR OF NATIONAL INTELLIGENCE
Case No. C 06-0672-JCS

Case 3:06-cv-00672-VRW Document 124-2 Filed 05/13/2006 Page 5 of 7

1 United States.

2 10. Through this declaration, I also invoke and assert a statutory privilege held by the
3 DNI under the National Security Act to protect intelligence sources and methods implicated by
4 this case. See 50 U.S.C. § 403-1(i)(1). My assertion of this statutory privilege for intelligence
5 information and sources and methods is coextensive with my state secrets privilege assertion.

6 **INFORMATION SUBJECT TO CLAIMS OF PRIVILEGE**

7 11. In an effort to counter the al Qaeda threat, the President of United States
8 authorized the NSA to utilize its SIGINT capabilities to collect certain "one-end foreign"
9 communications where one party is associated with the al Qaeda terrorist organization for the
10 purpose of detecting and preventing another terrorist attack on the United States. This activity is
11 known as the Terrorist Surveillance Program ("TSP"). To discuss this activity in any greater
12 detail, however, would disclose classified intelligence information and reveal intelligence
13 sources and methods, which would enable adversaries of the United States to avoid detection by
14 the U.S. Intelligence Community and/or take measures to defeat or neutralize U.S. intelligence
15 collection, posing a serious threat of damage to the United States' national security interests.
16 Thus, any further elaboration on the public record concerning the TSP would reveal information
17 that could cause the very harms my assertion of the state secrets privilege is intended to prevent.
18 The classified declaration of General Alexander that I considered in making this privilege
19 assertion, as well as my own separate classified declaration, provide a more detailed explanation
20 of the information at issue and the harms to national security that would result from its
21 disclosure.

22 12. Plaintiffs also make allegations regarding other purported activities of the NSA,
23 including allegations about NSA's purported involvement with AT&T. The United States can
24 neither confirm nor deny allegations concerning intelligence activities, sources, methods,
25 relationships, or targets. For example, disclosure of those who are targeted by such activities
26 would compromise the collection of intelligence information just as disclosure of those who are

27 DECLARATION OF JOHN D. NEGROPONTE,
28 DIRECTOR OF NATIONAL INTELLIGENCE
Case No. C 06-0672-JCS

1 not targeted would reveal to adversaries that certain communications channels are secure or,
2 more broadly, would tend to reveal the methods being used to conduct surveillance. The only
3 recourse for the Intelligence Community and, in this case, for the NSA, is to neither confirm nor
4 deny these sorts of allegations, regardless of whether they are true or false. To say otherwise
5 when challenged in litigation would result in routine exposure of intelligence information,
6 sources, and methods and would severely undermine surveillance activities in general. Thus, as
7 with the other categories of information discussed in this declaration, any further elaboration on
8 the public record concerning these matters would reveal information that could cause the very
9 harms my assertion of the state secrets privilege is intended to prevent. The classified
10 declaration of General Alexander that I considered in making this privilege assertion, as well as
11 my own separate classified declaration, provide a more detailed explanation of the information at
12 issue, the reasons why it is implicated by Plaintiffs' claims, and the harms to national security
13 that would result from its disclosure.

14 CONCLUSION

15 13. In sum, I formally invoke and assert the state secrets privilege, as well as a
16 statutory privilege under the National Security Act, to prevent the disclosure of the information
17 detailed in the two classified declarations that are available for the Court's *in camera* and *ex*
18 *parte* review. Moreover, because proceedings in this case risk disclosure of privileged and
19 classified intelligence-related information, I join with General Alexander in respectfully
20 requesting that the Court dismiss this case to stem the harms to the national security of the
21 United States that will occur if it is litigated.

22
23
24
25
26
27 DECLARATION OF JOHN D. NEGROPONTE,
28 DIRECTOR OF NATIONAL INTELLIGENCE
Case No. C 06-0672-JCS

1 I declare under penalty of perjury that the foregoing is true and correct.

2

3 DATE: 5/12/2006

John D. Negroponte
JOHN D. NEGROPONTE
Director of National Intelligence

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

DECLARATION OF JOHN D. NEGROPONTE,
DIRECTOR OF NATIONAL INTELLIGENCE
Case No. C 06-0672-JCS

28

EXHIBIT G

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

TASH HEPTING, GREGORY HICKS)
CAROLYN JEWEL and ERIK KNUTZEN)
on Behalf of Themselves and All Others)
Similarly Situated,)
Plaintiffs,)
v.)
AT&T CORP., AT&T INC. and)
DOES 1-20, inclusive,)
Defendants.)

Case No. C-06-0672-VRW

**DECLARATION OF
LIEUTENANT GENERAL
KEITH B. ALEXANDER, DIRECTOR,
NATIONAL SECURITY AGENCY**

I, Keith B. Alexander, declare as follows:

INTRODUCTION

1. I am the Director of the National Security Agency (NSA), an intelligence agency within the Department of Defense. I am responsible for directing the NSA, overseeing the operations undertaken to carry out its mission and, by specific charge of the President and the Director of National Intelligence, protecting NSA activities and intelligence sources and methods. I have been designated an original TOP SECRET classification authority under Executive Order No. 12958, 60 Fed. Reg. 19825 (1995), as amended on March 25, 2003, and Department of Defense Directive No. 5200.1-R, Information Security Program Regulations, 32 C.F.R. § 159a.12 (2000).

2. The purpose of this declaration is to support the assertion of a formal claim of the military and state secrets privilege (hereafter "state secrets privilege"), as well as a statutory privilege, by the Director of National Intelligence (DNI) as the head of the intelligence community. In this declaration, I also assert a statutory privilege with respect to information about NSA activities. For the reasons described below, and in my classified declaration

DECLARATION OF LT. GEN. KEITH B. ALEXANDER,
DIRECTOR, NATIONAL SECURITY AGENCY
Case No. C 06-0672-JCS

1 provided separately to the court for *in camera* and *ex parte* review, the disclosure of the
2 information covered by these privilege assertions would cause exceptionally grave damage to the
3 national security of the United States. The statements made herein, and in my classified
4 declaration, are based on my personal knowledge of NSA operations and on information made
5 available to me as Director of the NSA.

6 **THE NATIONAL SECURITY AGENCY**

7 3. The NSA was established by Presidential Directive in 1952 as a separately
8 organized agency within the Department of Defense. Under Executive Order 12333, § 1.12.(b),
9 as amended, NSA's cryptologic mission includes three functions: (1) to collect, process, and
10 disseminate signals intelligence ("SIGINT") information, of which communications intelligence
11 ("COMINT") is a significant subset, for (a) national foreign intelligence purpose, (b)
12 counterintelligence purposes, and (c) the support of military operations; (2) to conduct
13 information security activities; and (3) to conduct operations security training for the U.S.
14 Government.

15 4. There are two primary reasons for gathering and analyzing intelligence
16 information. The first, and most important, is to gain information required to direct U.S.
17 resources as necessary to counter external threats. The second reason is to obtain information
18 necessary to the formulation of the United States' foreign policy. Foreign intelligence
19 information provided by NSA is thus relevant to a wide range of important issues, including
20 military order of battle; threat warnings and readiness; arms proliferation; terrorism; and foreign
21 aspects of international narcotics trafficking.

22 5. In the course of my official duties, I have been advised of this litigation and
23 reviewed the allegations in Plaintiffs' Amended Complaint and Motion for a Preliminary
24 Injunction. As described herein and in my separate classified declaration, information
25 implicated by Plaintiffs' claims is subject to the state secrets privilege assertion in this case by
26 the DNI. The disclosure of this information reasonably could be expected to cause exceptionally

27 DECLARATION OF LT. GEN. KEITH B. ALEXANDER,
28 DIRECTOR, NATIONAL SECURITY AGENCY
Case No. C 06-0672-JCS

1 grave damage to the national security of the United States. In addition, it is my judgment that
2 any attempt to proceed in the case will substantially risk disclosure of the privileged information
3 and will cause exceptionally grave damage to the national security of the United States.

4 6. Through this declaration, I also hereby invoke and assert NSA's statutory
5 privilege to protect information related to NSA activities described below and in more detail in
6 my classified declaration. NSA's statutory privilege is set forth in section 6 of the National
7 Security Agency Act of 1959 (NSA Act), Public Law No. 86-36 (codified as a note to 50 U.S.C.
8 § 402). Section 6 of the NSA Act provides that "[n]othing in this Act or any other law . . . shall
9 be construed to require the disclosure of the organization or any function of the National
10 Security Agency [or] any information with respect to the activities thereof. . . ." By this
11 language, Congress expressed its determination that disclosure of any information relating to
12 NSA activities is potentially harmful. Section 6 states unequivocally that, notwithstanding
13 *any* other law, NSA cannot be compelled to disclose *any* information with respect to its
14 authorities. Further, NSA is not required to demonstrate specific harm to national security when
15 invoking this statutory privilege, but only to show that the information relates to its activities.
16 Thus, to invoke this privilege, NSA must demonstrate only that the information to be protected
17 falls within the scope of section 6. NSA's functions and activities are therefore protected from
18 disclosure regardless of whether or not the information is classified.

19 **INFORMATION SUBJECT TO CLAIMS OF PRIVILEGE**

20 7. Following the attacks of September 11, 2001, the President of United States
21 authorized the NSA to utilize its SIGINT capabilities to collect certain "one-end foreign"
22 communications where one party is associated with the al Qaeda terrorist organization under the
23 Terrorist Surveillance Program (TSP) for the purpose of detecting and preventing another
24 terrorist attack on the United States. Any further elaboration on the public record concerning the
25 TSP would reveal information that could cause the very harms that the DNI's assertion of the
26 state secrets privilege is intended to prevent. My separate classified declaration provides a more

27 DECLARATION OF LT. GEN. KEITH B. ALEXANDER,
28 DIRECTOR, NATIONAL SECURITY AGENCY
Case No. C 06-0672-JCS

1 detailed explanation of the information at issue and the harms to national security that would
2 result from its disclosure.

3 8. Plaintiffs also make allegations regarding other purported activities of the NSA,
4 including allegations about the NSA's purported involvement with AT&T. Regardless of
5 whether these allegations are accurate or not, the United States can neither confirm nor deny
6 alleged NSA activities, relationships, or targets. To do otherwise when challenged in litigation
7 would result in the exposure of intelligence information, sources, and methods and would
8 severely undermine surveillance activities in general. For example, if the United States denied
9 allegations about intelligence targets in cases where such allegations were false, but remained
10 silent in cases where the allegations were accurate, it would tend to reveal that the individuals in
11 the latter cases were targets. Any further elaboration on the public record concerning these
12 matters would reveal information that could cause the very harms that the DNI's assertion of the
13 state secrets privilege is intended to prevent. My separate classified declaration provides a more
14 detailed explanation of the information at issue and the harms to national security that would
15 result from its disclosure.

16 **CONCLUSION**

17 9. In sum, I support the DNI's assertion of the state secrets privilege and statutory
18 privilege to prevent the disclosure of the information detailed in my classified declaration that is
19 available for the Court's *in camera* and *ex parte* review. I also assert a statutory privilege with
20 respect to information about NSA activities. Moreover, because proceedings in this case risk
21 disclosure of privileged and classified intelligence-related information, I respectfully request that
22 the Court not only protect that information from disclosure, but also dismiss this case to stem the
23 harms to the national security of the United States that will occur if it is litigated.

24
25
26
27 DECLARATION OF L.T. GEN. KEITH B. ALEXANDER,
28 DIRECTOR, NATIONAL SECURITY AGENCY
Case No. C 06-0672-JCS

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

I declare under penalty of perjury that the foregoing is true and correct.

DATE: 12 May 06



LT. GEN. KEITH B. ALEXANDER
Director, National Security Agency

EXHIBIT H

1 DAVID L. ANDERSON #149604
JACOB R. SORENSEN #209134
2 BRIAN J. WONG #226940
50 Fremont Street
3 Post Office Box 7880
San Francisco, CA 94120-7880
4 Telephone: (415) 983-1000
Facsimile: (415) 983-1200
5 Email: bruce.ericson@pillsburylaw.com

6 SIDLEY AUSTIN LLP
DAVID W. CARPENTER (admitted *pro hac vice*)
7 DAVID L. LAWSON (admitted *pro hac vice*)
BRADFORD A. BERENSON (admitted *pro hac vice*)
8 EDWARD R. McNICHOLAS (admitted *pro hac vice*)
1501 K Street, N.W.
9 Washington, D.C. 20005
Telephone: (202) 736-8010
10 Facsimile: (202) 736-8711
Email: bberenson@sidley.com

11 Attorneys for Defendants
12 AT&T CORP. and AT&T INC.

13 UNITED STATES DISTRICT COURT
14 NORTHERN DISTRICT OF CALIFORNIA
15 SAN FRANCISCO DIVISION

16 TASH HEPTING, GREGORY HICKS,
17 CAROLYN JEWEL and ERIK KNUTZEN
on Behalf of Themselves and All Others
18 Similarly Situated,

19 Plaintiffs,

20 vs.

21 AT&T CORP., AT&T INC. and DOES 1-20,
22 inclusive,

23 Defendants.

No. C-06-0672-VRW

**REPLY MEMORANDUM OF
DEFENDANT AT&T CORP. IN
RESPONSE TO COURT'S MAY 17,
2006 MINUTE ORDER**

24 [REDACTED]

25

26

27

28

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

TABLE OF CONTENTS

PAGE

I. INTRODUCTION..... 1

II. ARGUMENT.3

A. The Government’s State Secrets Motion Cannot Properly Be Resolved Without Reviewing The Classified Submissions.3

1. Deciding A State Secrets Motion Routinely Entails Ex Parte Review Of Classified Submissions. 4

2. Due Process Is Not Violated By Such Review..... 8

3. The Provisions Of FISA Governing Disclosure Of FISA Materials Have No Application Here. 10

B. The Court Cannot Adjudicate Plaintiffs’ Prima Facie Claims Until It Reviews The Classified Submissions. 12

C. Plaintiffs Cannot Obtain Any Discovery Or Litigate Any Facts Relating To AT&T’s Immunity Before This Court Has Resolved The Government’s State Secrets Motion. 15

III. CONCLUSION. 20

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

TABLE OF AUTHORITIES

FEDERAL CASES

ACLU Foundation of Southern California v. Barr, 952 F.2d 457 (D.C. Cir. 1991)..... 11

Azzouka v. Meese, 820 F.2d 585 (2d Cir. 1987).....8

Azzouka v. Sava, 777 F.2d 68 (2d Cir. 1985)8

Black v. United States, 62 F.3d 1115 (8th Cir. 1995)..... 6

Dorfmont v. Brown, 913 F.2d 1399 (9th Cir. 1990).....6

DTM Research, L.L.C. v. AT&T Corp., 245 F.3d 327 (4th Cir. 2001)..... 11, 12

Ellsberg v. Mitchell, 709 F.2d 51 (D.C. Cir. 1983)..... 4, 6, 7

Fitzgerald v. Penthouse International, Ltd., 776 F.2d 1236 (4th Cir. 1985) 5, 6

Frost v. Perry, 161 F.R.D. 434 (D. Nev. 1995)..... 17

Global Relief Foundation v. O'Neill, 315 F.3d 748 (7th Cir. 2002)..... 8

In re Grand Jury Proceedings, 867 F.2d 539 (9th Cir. 1988).....9

Guenther v. Commissioner of Internal Rev. (Guenther I), 889 F.2d 882 (9th Cir. 1989).....9

Guenther v. Commissioner of Internal Rev. (Guenther II), 939 F.2d 758 (9th Cir. 1989).....9

Halkin v. Helms, 598 F.2d 1 (D.C. Cir. 1978)..... 6, 14,15

Halkin v. Helms, 690 F.2d 977 (D.C. Cir. 1982).....5

Halperin v. Kissinger, 424 F. Supp. 838 (D.D.C. 1976), *rev'd on other grounds*, 606 F.2d 1192 (D.C. Cir. 1979)..... 18

Holy Land Foundation for Relief & Development v. Ashcroft, 333 F.3d 156 (D.C. Cir. 2003)..... 8

Jay v. Boyd, 351 U.S. 345 (1956).....8

Jifry v. Federal Aviation Admin., 370 F.3d 1174 (D.C. Cir. 2004)..... 8

Joint Anti-Fascist Refugee Commission v. McGrath, 341 U.S. 123 (1951).....9

Kasza v. Browner, 133 F.3d 1159 (9th Cir. 1998) 4-6, 16-17

1 *Lynn v. Regents of University Calif.*, 656 F.2d 1337 (9th Cir. 1981)..... 9

2 *Meridian International Logistics, Inc. v. United States*, 939 F.2d 740 (9th Cir. 1991) 9

3 *National Council of Resistance of Iran v. Department of State*, 251 F.3d 192 (D.C.

4 Cir. 2001)..... 8

5 *National Council of Resistance of Iran v. Department of State*, 373 F.3d 152 (D.C.

6 Cir. 2004)..... 8

7 *Nixon v. Sirica*, 487 F.2d 700 (D.C. Cir. 1973)..... 7

8 *People's Mojahedin Organization of Iran v. Department of State*, 327 F.3d 1238

9 (D.C. Cir. 2003)..... 8

10 *Pollard v. Federal Bureau of Investigation*, 705 F.2d 1151 (9th Cir. 1983)..... 9

11 *Shaughnessy v. United States ex rel. Mezel*, 345 U.S. 206 (1953)..... 8

12 *Smith v. Nixon*, 606 F.2d 1183 (D.C. Cir. 1979)..... 19

13 *Suciu v. Immig. and Naturalization Services*, 755 F.2d 127 (8th Cir. 1985) 8

14 *United States ex rel. Barbour v. District Director of the INS*, 491 F.2d 573 (5th Cir.

15 1974)..... 8

16 *United States v. Belfield*, 692 F.2d 141 (D.C. Cir. 1982)..... 11

17 *United States v. Ott*, 637 F. Supp. 62 (E.D. Cal. 1986)..... 11

18 *United States v. Ott*, 827 F.2d 473 (9th Cir. 1987)..... 9

19 *United States v. Reynolds*, 345 U.S. 1 (1953) 4-5

20 *United States v. Sarkissan*, 841 F.2d 959 (9th Cir. 1988) 9

21 *United States v. Shaughnessy*, 338 U.S. 537 (1950) 8

22 *United States v. Spanjol*, 720 F. Supp. 55 (E.D. Pa. 1989)..... 11

23 *United States v. Thomson*, 752 F. Supp. 75 (W.D.N.Y. 1990)..... 11

24 *Zuckerbraun v. General Dynamics Corp.*, 935 F.2d 544 (2d Cir. 1991) 5

25 **FEDERAL STATUTES**

26 50 U.S.C. § 1801 14

27 50 U.S.C. § 1806 2, 10, 11

28

1 50 U.S.C. § 1845 2, 10, 11
2 47 U.S.C. § 2511 3, 15, 17
3 18 U.S.C. § 2510 14
4 18 U.S.C. § 2702 14

5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

1 Defendants AT&T Inc. and AT&T Corp. (collectively "AT&T") respectfully submit
2 this reply memorandum addressing the two issues raised in the Court's Minute Order of
3 May 17, 2006 ("Minute Order," Dkt. 130): (1) whether this case can be litigated without
4 deciding the state secrets issue, thus obviating any need for the Court to review the
5 government's classified submissions and (2) whether plaintiffs are entitled to discovery of
6 any authorizations the government may have provided to AT&T notwithstanding the
7 government's invocation of the state secrets privilege.

8 **I. INTRODUCTION.**

9 In their Memorandum in Response to the Minute Order, plaintiffs maintain that this
10 case can proceed without the Court deciding the state secrets issue and that, accordingly,
11 the Court should not even *look at* the government's classified submissions in support of its
12 assertion of the military and state secrets privilege in this case. Plaintiffs ignore that the
13 classified portions of the government's Motion to Dismiss ("Government's Motion," Dkts.
14 124 – 125) are, as the Court recognized at the hearing on May 17, 2006, "the heart of [the
15 government's] argument" in support of its Motion. Tr. of May 17th Hearing, at 33.11-12.

16 Plaintiffs advance a number of arguments in support of their claim that the Court
17 should not review the government's classified submissions. First, they contend that due
18 process "disfavors" the consideration of evidence in *ex parte, in camera* proceedings.
19 Plaintiffs do not argue that such proceedings actually *violate* due process, and for good
20 reason. Decades of decisions establish that *ex parte, in camera* review of classified
21 submission is the standard and appropriate means of evaluating state secrets assertions and
22 that the only course of action that would deny due process would be allowing plaintiffs to
23 impose massive liabilities on AT&T when AT&T is barred by the government's assertion
24 of the state secrets privilege from rebutting plaintiff's allegations.

25 Plaintiffs also contend that if the Court is going to review the government's *ex*
26 *parte, in camera* submissions, two sections of the Foreign Intelligence Surveillance Act
27 ("FISA") give plaintiffs the right to review them, too. This contention ignores that the
28 provisions of FISA they cite – 50 U.S.C. § 1806(f); 50 U.S.C. § 1845(f) – are intended to

1 apply mainly when the government seeks to use evidence obtained through FISA warrants
2 against individuals whose communications were intercepted pursuant to FISA. Because
3 plaintiffs have specifically alleged that the purported surveillance they are challenging did
4 not occur pursuant to FISA, *see* First Amended Complaint (“FAC”) ¶¶ 2, 35, they cannot
5 and have not alleged that they were subjected to government surveillance (pursuant to FISA
6 or otherwise). As such, the FISA provisions they cite offer no support to their claim to
7 review the government’s classified submissions. Notably, however, those provisions
8 provide that, even in an FISA case, courts may perform the sort of *ex parte* and *in camera*
9 review of classified information that plaintiffs resist here.

10 Plaintiffs next assert that the Court can adjudicate plaintiffs’ claims without resort to
11 the classified information the government has submitted in support of its Motion to
12 Dismiss. In its public filings, the United States explained in detail that no aspect of
13 plaintiffs’ cause of action – from plaintiffs’ standing, to the elements of its statutory causes
14 of action, to the elements of its Fourth Amendment claims – can be proven by plaintiffs or
15 defended against by AT&T without invading the domain protected by the constitutionally-
16 grounded state secrets doctrine.¹ *See* Gov’t Mem. at 16 (“every step in this case . . . runs
17 into privileged information”). Yet plaintiffs maintain that the Court need take no account
18 of the underlying basis for this explanation before rejecting it. Plaintiffs, of course, cannot
19 discern the specific relevance or significance of this information, and so they cannot say
20 whether the information would in fact bear on the litigation of their claims. Only the Court
21 can make that determination. It should go without saying that the Court can only do so
22 after it has actually reviewed the information. If the information is in fact relevant to
23 plaintiffs’ claims, the Court cannot permit the case to proceed against AT&T. Because of

24
25 ¹ Gov’t Mem. at 16-23 (plaintiffs standing); at 21 (whether AT&T has intentionally
26 intercepted or disclosed the contents of plaintiffs communications or calling record or
27 related information); at 21-23, 28 (whether any interceptions or related activities were in
28 accord with certifications of the Attorney General or other authorizations that confer
immunity on carriers from *any* cause of action); at 23-28 (plaintiffs’ Fourth Amendment
claims).

1 the government's assertion of the state secrets privilege, AT&T cannot defend itself against
2 plaintiffs' claims. Plaintiffs' argument that the Court could decide this case without
3 examining the foundation for the government's state secrets assertion defies common sense.

4 Finally, plaintiffs argue that the statute that would provide AT&T with immunity
5 from plaintiffs' suit (18 U.S.C. § 2511(2)(a)(ii)) somehow mandates discovery of any
6 authorization AT&T may have received from the government for assisting it with alleged
7 surveillance activities. Section 2511(2)(a)(ii) says nothing of the sort. To the contrary, it
8 prevents telecommunications providers such as AT&T from disclosing any such
9 certifications "except as may otherwise be required by legal process." 47 U.S.C. §
10 2511(2)(a)(ii). Because there is no such "otherwise required" legal process at issue here,
11 plaintiffs' claim to discovery of government certifications – the mere existence of which
12 section 2511(2)(a)(ii) prevents AT&T from either confirming or denying – falls flat.

13 **II. ARGUMENT.**

14 **A. The Government's State Secrets Motion Cannot Properly Be Resolved Without**
15 **Reviewing The Classified Submissions.**

16 Ensuring proper application of the state secrets doctrine is primarily the province
17 and concern of the United States. AT&T offers its views on this subject in response to the
18 Court's invitation in the Minute Order of May 17 to the extent that such views may be of
19 assistance to the Court.

20 Contrary to plaintiffs' arguments, AT&T does not believe that an assertion of state
21 secrets by the United States may blithely be dismissed without even considering the basis
22 for it. Assertions of state secrets must be made personally by the nation's most senior
23 intelligence officials, as they were here. To the extent courts can ever rule on state secrets
24 assertions without examining the government's supporting submissions, it is only to accept
25 such assertions where the potential for compromising state secrets is obvious. Where there
26 is any doubt, *ex parte* and *in camera* review of classified submissions is the standard and
27 accepted method for adjudicating state secrets issues. To render the rulings plaintiffs seek

28

1 without even reviewing the evidence tendered personally to this Court by the Director of
2 National Intelligence and Director of the National Security Agency would be
3 unprecedented and wrong. Regardless of what the government's classified submissions
4 contain – something we do not know – the better course is to review those submissions
5 before deciding whether this case may proceed.

6 **1. Deciding A State Secrets Motion Routinely Entails Ex Parte Review Of**
7 **Classified Submissions.**

8 The state secrets privilege allows the government to prevent the unauthorized
9 disclosure of information during litigation that might harm national security interests. *See,*
10 *e.g., United States v. Reynolds*, 345 U.S. 1, 7-8 (1953); *Kasza v. Browner*, 133 F.3d 1159,
11 1166 (9th Cir. 1998); *Ellsberg v. Mitchell*, 709 F.2d 51, 57 (D.C. Cir. 1983) (“the various
12 harms against which protection is sought by invocation of the privilege, include[e]
13 impairment of the nation's defense capabilities [and] disclosure of intelligence-gathering
14 methods or capabilities”). The invocation of state secrets must be made formally through
15 an affidavit by “the head of the department which has control over the matter, after actual
16 personal consideration by the officer.” *Reynolds*, 345 U.S. at 7-8. The judgment of such
17 officers, who are constitutionally entrusted and empowered to protect the nation's security,
18 is due the “utmost deference” by the courts, and the scope of a reviewing court's discretion
19 to reject them is exceedingly narrow. *Id.* at 10; *see also Kasza*, 133 F.3d at 1166. A court
20 that does not review the government's filing cannot be giving proper consideration or
21 deference to the government's position. “Once the privilege is properly invoked and the
22 court is satisfied as to the danger of divulging state secrets, the privilege is absolute,” and
23 “even the most compelling necessity cannot overcome the claim of privilege.” *Kasza*, 133
24 F.3d at 1166-7 (quoting *Reynolds*, 345 U.S. at 11 n.26).

25 Where, as here, the government contends that “the ‘very subject matter of the
26 action’ is a state secret,” the Court must “dismiss the plaintiff's action based solely on the
27 invocation of the state secrets privilege” as long as “the court is ultimately satisfied that

28

1 there are military secrets at stake.” *Kasza*, 133 F.3d at 1166 (quoting *Reynolds*, 345 U.S.
2 at 11 n.26); *see also Black v. United States*, 62 F.3d 1115 (8th Cir. 1995); *Fitzgerald v.*
3 *Penthouse Internat’l, Ltd.*, 776 F.2d 1236, 1239, 1241-42 (4th Cir. 1985); *Halkin v. Helms*,
4 690 F.2d 977, 999 (D.C. Cir. 1982). “While dismissal of an action based on the state
5 secrets privilege is harsh, the results are harsh in either direction and the state secrets
6 doctrine finds the greater public good – ultimately the less harsh remedy – to be dismissal.”
7 *Kasza*, at 1167 (quoting *Bareford v. General Dynamics Corp.*, 973 F.2d 1138, 1144 (5th
8 Cir. 1992)).

9 In limited circumstances, state secrets assertions may be adjudicated without
10 reviewing the underlying state secrets information – but only where the government’s
11 assertion is accepted. In *United States v. Reynolds*, 345 U.S. 1 (1953), the Supreme Court
12 indicated that:

13 It may be possible to satisfy the court, from all the
14 circumstances of the case, that there is a reasonable danger
15 that compulsion of the evidence will expose military matters
16 which, in the interest of national security, should not be
17 divulged. When this is the case, the occasion for the privilege
18 is appropriate, and the court should not jeopardize the
19 security which the privilege is meant to protect by insisting
20 upon an examination of the evidence, even by the judge
21 alone, in chambers.

22 *Id.* at 10; *see also Zuckerbraun v. General Dynamics Corp.*, 935 F.2d 544 (2d Cir. 1991)
23 (accepting privilege assertion without *in camera* review). Short of such a situation,
24 however, a reviewing court is obliged to satisfy itself that the threshold for proper
25 invocation of the privilege has been met – *i.e.*, “that there is a reasonable danger that
26 compulsion of the evidence will expose military matters which, in the interest of national
27 security, should not be divulged.” *Kasza*, 133 F.3d at 1166 (internal quotations omitted).
28 Once such a determination is made, the court’s job is at an end; the privilege is absolute and
cannot be overcome by any countervailing considerations. *See id.*

1 The standard and accepted means for a court to satisfy itself that the threshold has
2 been met is through *ex parte* and *in camera* review of privileged and/or classified
3 submissions by the government. *See, e.g., Kasza*, 133 F.3d at 1169; *Black v. United States*,
4 62 F.3d 1115, 1119 (8th Cir. 1995); *Fitzgerald v. Penthouse Internat'l, Ltd.*, 776 F.2d 1236
5 (4th Cir. 1985); *Halkin v. Helms*, 598 F.2d 1, 3 (D.C. Cir. 1978) (“It is settled that in
6 camera proceedings are an appropriate means to resolve disputed issues of privilege”). As
7 a practical matter, how else can the Court determine whether the privilege has been
8 properly invoked? The clear answer is the Court cannot. Neither plaintiff nor defendant
9 is empowered or entrusted to review or comment on the privileged submission; both are
10 equally disabled from having access to national security secrets that, by definition, they are
11 not authorized to possess. *Cf., e.g., Dorfmont v. Brown*, 913 F.2d 1399 (9th Cir. 1990)
12 (courts lack jurisdiction to interfere in security clearance determinations). Instead, only the
13 court is constitutionally entrusted with the responsibility to verify the bona fides of the
14 executive’s assertion of state secrets. Such verification necessarily entails review of the
15 government’s *ex parte, in camera* submission. Not surprisingly, plaintiffs are unable to cite
16 even a single case in which a reviewing court has rejected a state secrets submission
17 without reviewing it.

18 Nor is plaintiffs’ effort to convince this Court that review of the classified
19 submission is a last resort—to be undertaken only if the government makes a
20 “particularized showing” of state secrets and the court determines “what information
21 properly falls within and without the state secrets privilege”—any more availing. The
22 whole purpose of the classified submission is to make the “particularized showing”
23 plaintiffs seek, such that the court can make the determination they request. To ask that the
24 government make public more of the information it is trying to keep secret or that the court
25 evaluate privilege claims and resolve discovery requests without access to the privileged
26 information is unreasonable and incorrect.

27

28

1 *Ellsberg v. Mitchell*, 709 F.2d 51 (D.C. Cir. 1983), and *Nixon v. Sirica*, 487 F.2d
2 700 (D.C. Cir. 1973) (en banc), mandate no such result. *Ellsberg* rejected “a strict rule that
3 the trial judge must compel the government to defend its claim publicly before submitting
4 materials *in camera*,” *id.* at 63, holding only that “the trial judge should insist (1) that the
5 formal claim of privilege be made on the public record and (2) that the government either
6 (a) publicly explain in detail the kinds of injury to national security it seeks to avoid and the
7 reason those harms would result from revelation of the requested information or (b) indicate
8 why such an explanation would itself endanger national security,” *id.* at 63-64. The
9 government’s extensive submissions in this case easily satisfy this standard.

10 The *Ellsberg* court went out of its way “to make clear the limitations of our ruling:
11 The government’s public statement need be no more (and no less) specific than is
12 practicable under the circumstances.” *Id.* at 64. And even this rule only applied in a
13 limited class of cases, totally unlike this one, where “the surrounding circumstances did not
14 make apparent the likelihood that disclosure would lead to serious injury,” *id.* at 61 – there,
15 because the surveillance at issue had admittedly stopped more than five years earlier. And
16 *Nixon* involved the wholly different context of a criminal prosecution of executive branch
17 officials, in which, in effect, the executive branch was on both sides of the case. The court
18 there rejected the notion that any public explanation had to be given regarding materials
19 that “relate[] to national defense or foreign relations.” 487 F.2d at 721.

20 If the state secrets assertion in this case could be decided without recourse to the
21 government’s classified submission, it could only be decided in favor of the government:
22 the threat to national security is obvious from permitting litigation of claims that, on their
23 face, place in issue the details of a highly classified intelligence program and almost
24 nothing else. But, unless this Court grants AT&T’s motion to dismiss on non-state secrets
25 grounds, thereby avoiding the need to confront this issue at all, the better course of action is
26 for this Court to review the classified information the government has made available to it
27 for *ex parte* and *in camera* review.

28

1 **2. Due Process Is Not Violated By Such Review.**

2 Although plaintiffs do not directly contend that due process would be violated by *in*
3 *camera*, *ex parte* review of the government's classified submissions in this case, they
4 nevertheless attempt to bolster their arguments by vague allusions to due process: its
5 general requirements, its "very spirit," and its "disfavor" for "secret evidence [and]
6 arguments." Plaintiffs' Memorandum ("Pltfs. Mem.") at 2-3. Plaintiffs' due process
7 concerns are misplaced in the context of this case. As detailed above, numerous courts,
8 including the Ninth Circuit, have found that review of *in camera*, *ex parte* classified
9 submissions is an appropriate procedure for determining whether a case can proceed after
10 invocation of the state secrets privilege. *See supra* Section II.A.1. Moreover, due process
11 claims have been consistently rejected in analogous contexts involving *in camera*, *ex parte*
12 review of classified submissions, including cases reviewing blocking orders issued under
13 the International Emergency Economic Powers Act ("IEEPA"),² designations of "foreign
14 terrorist organizations" under the Anti-Terrorism and Effective Death Penalty Act
15 ("AEDPA"),³ and immigration deportation proceedings.⁴

16

17 ² *See, e.g., Holy Land Found. for Relief & Dev. v. Ashcroft*, 333 F.3d 156, 164 (D.C. Cir.
18 2003), cert. denied 540 U.S. 1218 (2004); *Global Relief Found. v O'Neill*, 315 F.3d 748,
19 754 (7th Cir. 2002).

19 ³ *See, e.g., National Council of Resistance of Iran v. Dep't of State*, 373 F.3d 152, 158
20 (D.C. Cir. 2004); *People's Mojahedin Organization of Iran v. Dep't of State*, 327 F.3d
21 1238, 1242 (D.C. Cir. 2003); *National Council of Resistance of Iran v. Dep't of State*, 251
22 F.3d 192, 208 (D.C. Cir. 2001); *see also Jifry v. Fed. Aviation Admin.*, 370 F.3d 1174,
23 1184 (D.C. Cir. 2004) (holding that the same due process protections that apply to
24 terrorism listing cases under AEDPA also apply to FAA revocation of airmen certificates
25 based on finding that pilots posed a security risk and rejecting argument that pilots' due
26 process rights were violated because they did not have access to the specific, classified
27 evidence on which the agency relied in making its determination), cert. denied 543 U.S.
28 1146 (2005).

24 ⁴ *See, e.g., Suciu v. Immig. and Naturalization Servs.*, 755 F.2d 127, 128 (8th Cir. 1985);
25 *United States ex rel. Barbour v. District Director of the INS*, 491 F.2d 573, 578 (5th Cir.
26 1974); *see also Jay v. Boyd*, 351 U.S. 345 (1956) (government may rely on classified
27 information to deny discretionary immigration relief); *Shaughnessy v. United States ex*
28 *rel. Mezel*, 345 U.S. 206 (1953) (government may rely on confidential information to
29 exclude an alien from the United States); *United States v. Shaughnessy*, 338 U.S. 537
30 (1950) (same); *Azzouka v. Meese*, 820 F.2d 585, 587 (2d Cir. 1987) (same); *Azzouka v.*
31 (continued...)

1 Plaintiffs make no attempt to come to grips with any of this law. Instead, they rely
2 on several due process cases from unrelated and inapposite contexts. In *Lynn v. Regents of*
3 *Univ. Calif.*, 656 F.2d 1337 (9th Cir. 1981), for example, a garden-variety gender
4 discrimination case, the court held that the district court's *in camera*, *ex parte* review of the
5 tenure file of the plaintiff professor violated due process. Similarly, in *Guenther v. Comm'r*
6 *of Internal Rev. (Guenther II)*, 939 F.2d 758 (9th Cir. 1991), an appeal by taxpayers of an
7 IRS finding of tax deficiency, the court held that the district court's *ex parte* consideration
8 of the agency's trial memorandum violated due process.⁵ It should come as no surprise that
9 neither *Lynn* nor *Guenther II* involved an assertion of the state secrets privilege or any
10 analogous national security consideration of the kind that has consistently led courts,
11 including the Ninth Circuit,⁶ to approve *ex parte*, *in camera* review of classified
12 information.⁷

13
14
15 (. . .continued)
Sava, 777 F.2d 68, 72 (2d Cir. 1985) (same).

16 ⁵ Plaintiffs also cite *Guenther v. Comm'r of Internal Rev. (Guenther I)*, 889 F.2d 882 (9th
17 Cir. 1989), a prior ruling in the same case in which the Ninth Circuit remanded the case
for an evidentiary hearing on the issue of the *ex parte* communication.

18 ⁶ See, e.g., *Meridian Internat'l Logistics, Inc. v. United States*, 939 F.2d 740, 745 (9th Cir.
19 1991) (holding that *ex parte* review of declaration concerning whether employee was
acting within the scope of his employment was proper and adequately balanced the rights
20 of the interested parties); *In re Grand Jury Proceedings*, 867 F.2d 539, 541 (9th Cir.
1988) (holding that party was not denied due process by district court's *in camera*
21 inspection of the materials upon which the government based its showing of the crime-
fraud exception); *United States v. Sarkissian*, 841 F.2d 959, 965 (9th Cir. 1988) (stating
22 that Classified Information Procedures Act permits *ex parte* submissions); *United States*
v. Ott, 827 F.2d 473, 476-77 (9th Cir. 1987) (holding that due process was not violated by
23 *ex parte*, *in camera* proceeding under Foreign Intelligence Surveillance Act); *Pollard v.*
Fed. Bureau of Investigation, 705 F.2d 1151, 1153-54 (9th Cir. 1983) (stating that
24 practice of *in camera*, *ex parte* review is appropriate in certain cases under the Freedom
of Information Act).

25 ⁷ Plaintiffs' reference to the principle articulated by Justice Frankfurter in his concurring
opinion in *Joint Anti-Fascist Refugee Comm'n v. McGrath*, 341 U.S. 123, 170 (1951), is
26 just generalized flag-waving; it provides no more concrete support than *Lynn* or *Guenther*
II for the proposition that due process concerns somehow alter the well-established
27 procedure for evaluating state secrets assertions by the United States in national security-
related litigation such as this.

28

1 **3. The Provisions Of FISA Governing Disclosure Of FISA Materials Have No**
2 **Application Here.**

3 Plaintiffs point to two sections of FISA – 50 U.S.C. §§ 1806(f), 1845(f) – in arguing
4 that if the Court is going to review the government’s *ex parte, in camera* submissions,
5 plaintiffs should also be able to do so. Pltfs. Mem.. at 4 (“[T]he Court should do so under
6 conditions that provide for some form of appropriate access by plaintiffs’ counsel.”). These
7 provisions of FISA are designed to apply primarily in circumstances in which the
8 government seeks to use evidence obtained through FISA warrants against individuals
9 whose communications were intercepted. Plaintiffs have specifically alleged that the
10 purported surveillance they are challenging did not occur pursuant to FISA, *see* FAC ¶¶ 2,
11 35; they cannot and have not alleged that they themselves were subjected to government
12 surveillance, pursuant to FISA or otherwise; and the government is not, in any event,
13 attempting to use information derived from surveillance of plaintiffs against them in this or
14 any other proceedings. *See* 50 U.S.C. § 1806(c) (1806(f) procedures apply, *inter alia*,
15 “[w]henver the Government intends to enter into evidence or otherwise use or disclose in
16 any trial, hearing, or other proceeding . . . against an aggrieved person, any information
17 obtained or derived from an electronic surveillance of that aggrieved person”). Absent a
18 broad expansion of the traditional understanding of the purpose of these provisions, they
19 lend no support to plaintiffs’ position.

20 Moreover, these FISA provisions specifically mandate the very thing plaintiffs are
21 attempting to resist: *ex parte* and *in camera* review. At most, Sections 1806(f) and 1845(f)
22 provide a court with some discretion to disclose to litigants certain evidence gathered
23 pursuant to FISA, but only after it first reviews the purported evidence *in camera* and *ex*
24 *parte*. *See* 50 U.S.C. § 1806(f) (District Court “shall . . . review *in camera* and *ex parte* the
25 application, order, and such other materials relating to the surveillance as may be
26 necessary to determine whether the surveillance of the aggrieved person was lawfully
27 authorized and conducted”) (emphasis added); 50 U.S.C. § 1845. Thus, plaintiffs’

28

1 threshold argument that the Court should not be able to review the government's
2 submissions flies in the face of the very statutes they cite.

3 Further, even if these provisions were applicable – which they are not – sections
4 1806(f) and 1845(f) provide only that a court *may* disclose the secret material. *See* 50
5 U.S.C. § 1806(f); 50 U.S.C. § 1845(f). Such disclosure is not mandatory, and plaintiffs cite
6 no case in which those provisions have been held to permit or require disclosure of state
7 secrets. Indeed, the great weight of authority interpreting the FISA sections plaintiffs cite
8 mandates that even ordinary FISA surveillance information over which no formal state
9 secrets claim has been asserted should not be disclosed. *See ACLU Foundation of Southern*
10 *California v. Barr*, 952 F.2d 457, 469 (D.C. Cir. 1991) (noting that 50 U.S.C. § 1806(f) “is
11 designed to prevent disclosure of information relating to FISA surveillance in adversary
12 proceedings”); *United States v. Belfield*, 692 F.2d 141, 147 (D.C. Cir. 1982) (rejecting
13 argument that disclosure was necessary and holding that under 1806(f) “[d]isclosure and an
14 adversary hearing are the exception, occurring *only* when necessary”) (emphasis in
15 original); *United States v. Thomson*, 752 F. Supp. 75, 79 (W.D.N.Y. 1990) (“No court that
16 has been required to determine the legality of a FISA surveillance has found disclosure or
17 an adversary hearing necessary”); *United States v. Spanjol*, 720 F. Supp. 55, 59 (E.D. Pa.
18 1989) (refusing to disclose information where “discovery would reveal the targets of
19 electronic surveillance, thereby compromising intelligence sources and methods”); *United*
20 *States v. Ott*, 637 F. Supp. 62, 65-66 (E.D. Cal. 1986) (noting that “[i]n the sensitive area of
21 foreign intelligence gathering, the need for extreme caution and sometimes even secrecy
22 may not be overemphasized” and holding that “there is no need for disclosure to protect the
23 respondent's legitimate interests”), *aff'd* 827 F.2d 473 (9th Cir. 1987).

24 In support of the argument that they should be able to review the government's
25 submissions, plaintiffs cite a case where the Court declined to disclose the state secrets at
26 issue. Pltfs. Mem. at 4 (citing *DTM Research, L.L.C. v. AT&T Corp.*, 245 F.3d 327 (4th
27 Cir. 2001)). In *DTM Research*, the government invoked the state secrets privilege in

28

1 support of its motion to quash third-party subpoenas. The district court granted the motion
2 to quash, and the Court of Appeals affirmed. Despite having protected the state secrets
3 information, the *DTM Research* court declined to dismiss the case because, unlike here, that
4 case was not one in which “the very question upon which the case turns is itself a state
5 secret, or the circumstances make clear that sensitive military secrets will be so central to
6 the subject matter of the litigation that any attempt to proceed will threaten disclosure of the
7 privileged matters.” 245 F.3d at 334 (internal quotations omitted). Instead, the state secrets
8 in that case were “not central” to the question of liability and could be excluded from trial
9 without fundamentally impairing the litigation. *Id.* Here, plaintiffs have alleged in their
10 complaint that AT&T has been authorized by the government to assist it with a secret
11 surveillance program. *Ipsa facto*, then, “the very question upon which the case turns is
12 itself a state secret,” *id.*, and the government has accordingly sought dismissal of the entire
13 action. *DTM Research* is irrelevant.

14 **B. The Court Cannot Adjudicate Plaintiffs’ Prima Facie Claims Until It Reviews**
15 **The Classified Submissions.**

16 Plaintiffs claim that their *prima facie* case can be fully presented and litigated based
17 solely on their existing evidence and that, therefore, this Court need not review any
18 classified materials to assess those claims. This argument fundamentally misconstrues the
19 state secrets doctrine, the significance of the Klein evidence, the law that would govern any
20 litigation of the merits of plaintiffs’ claims, and, most importantly, the effect the
21 government’s assertion of the state secrets privilege has on AT&T’s ability to defend itself
22 in this action.

23 Plaintiffs contend that the Klein Declaration is itself sufficient to make out a *prima*
24 *facie* case on their statutory claims. But even if one focused only on the two claims as to
25 which plaintiffs make any argument, the Court could not determine the validity of those
26 claims without first evaluating information covered by the government’s state secrets
27 assertion. [REDACTED]

28

1 [REDACTED]
2 [REDACTED]
3 [REDACTED]

4 AT&T cannot confirm or deny any of the facts on which plaintiffs' complaint is
5 based. But it is certain that the Klein Declaration and its associated exhibits are insufficient
6 to demonstrate any illegal conduct by AT&T. [REDACTED]

7 [REDACTED]
8 [REDACTED]
9 [REDACTED]
10 [REDACTED]
11 [REDACTED]

12 [REDACTED] Plaintiff's purported expert, of course,
13 has no knowledge whether this is true or not.

14 Even accepting their allegations as true, plaintiffs' declarations fail to establish their
15 claims. Key factual issues that bear directly on the viability of their legal claims and
16 AT&T's defenses are subject to the Government's state secrets assertion and are
17 unavailable. Without either confirming or denying the plaintiffs' assertions, [REDACTED]

18 [REDACTED]
19 [REDACTED]
20 [REDACTED]
21 [REDACTED]
22 [REDACTED]
23 [REDACTED]
24 [REDACTED]
25 [REDACTED]
26 [REDACTED]
27 [REDACTED]

28

1 [REDACTED]
2 [REDACTED]
3 [REDACTED]
4 [REDACTED]
5 [REDACTED]
6 [REDACTED]
7 [REDACTED]
8 [REDACTED]
9 [REDACTED]
10 [REDACTED]
11 [REDACTED]

12 Accordingly, without admitting or denying any factual assertions by the plaintiffs, it
13 is clear they lack even prima facie evidence of any governmental interception or electronic
14 surveillance of any communications – much less any illegal activity. No such evidence
15 could possibly be developed without delving deeply into matters covered by the
16 government’s existing state secrets assertion.

17 Plaintiffs’ request that this Court nonetheless proceed based on their “evidence” –
18 and only their evidence – is essentially a request that the Court presume guilt on the part of
19 AT&T. This is precisely the approach attempted in and rejected by *Halkin v. Helms*, 598
20 F.2d 1 (D.C. Cir. 1978), in which the Court refused to assume from the mere fact that
21 warrantless acquisitions of communications occurred that individuals on NSA watch lists
22 were actually being surveilled by the government. *Id.* at 10. There, as here, plaintiffs
23 attempted to circumvent the assertion of a state secrets privilege by asking the court to draw
24 unsupported inferences against private defendants, but the Court of Appeals recognized
25 that:

26 The underlying premise of the argument is that the defendants
27 should not be permitted to avoid liability for unconstitutional
28 acts by asserting a privilege which would prevent plaintiffs

1 from proving their case. The premise is faulty. The
2 defendants are not asserting the privilege to shield allegedly
3 unlawful actions; the state secrets privilege asserted here
4 belongs to the United States and is asserted by the United
5 States which is not a party to the action. It would be
6 manifestly unfair to permit a presumption of acquisition of
7 the watchlisted plaintiffs' international communications to run
8 against these defendants.

9 598 F.2d. at 10. As that court concluded, “[n]ot only would such a presumption be unfair to
10 the individual defendants who would have no way to rebut it, but it cannot be said that the
11 conclusion reasonably follows from its premise.” *Id.* Plaintiffs’ suggestion that they have
12 established a prima facie case requests exactly such a presumption and asks this Court to
13 draw unsupported factual and legal inferences AT&T would have no fair opportunity to
14 rebut in light the government’s state secrets assertion.

15 **C. Plaintiffs Cannot Obtain Any Discovery Or Litigate Any Facts Relating To**
16 **AT&T’s Immunity Before This Court Has Resolved The Government’s State**
17 **Secrets Motion.**

18 As Plaintiffs recognize, section 2511(2)(a)(ii) provides absolute statutory immunity
19 “[n]otwithstanding any other law” to any provider of wire or electronic communications
20 that provides the government with “information, facilities, or technical assistance” if such
21 provider has been provided with appropriate governmental authorizations. 18 U.S.C. §
22 2511(2)(a)(ii) (“No cause of action shall lie in any court against any provider or wire or
23 electronic communications . . . for providing information, facilities or assistance in
24 accordance with the terms of a . . . certification under this chapter”). And, as AT&T Corp.
25 has explained in its motion to dismiss, a provider of wire or electronic communications also
26 enjoys both absolute and qualified common-law immunity for alleged assistance to the
27 government that the government has assured the provider is lawful. *See* AT&T Motion at
28 13-19.

Plaintiffs are wrong in suggesting that the Court could adjudicate as a factual matter
the question whether AT&T has immunity from suit or allow discovery of any government

1 authorizations or assurances AT&T may have received without reviewing the government's
2 classified state secrets showing.⁸ As the government explained in its motion to dismiss, its
3 state secrets assertion "covers *any* information tending to confirm or deny" whether "AT&T
4 was involved with any" of the "alleged intelligence activities." Motion to Dismiss of the
5 United States at 17-18.

6 The existence or non-existence of any such government authorizations or assurances
7 is quite obviously information that would tend to confirm or deny AT&T's involvement
8 with the alleged government intelligence activities and is thus squarely within the
9 government's state secrets assertion. Accordingly, the Court could not adjudicate, or allow
10 discovery on, the alleged existence of any such authorizations or assurances without first
11 considering and rejecting the government's state secrets assertion. *See* Motion to Dismiss
12 of the United States at 23 ("even if Plaintiffs speculated and alleged the absence of section
13 2511(2)(a)(ii) authorization, they could not meet their burden of proof on the issue because
14 information confirming or denying AT&T's involvement in the alleged intelligence
15 activities is covered by the state secrets assertion"). And, as explained above, the Court
16 could not do that without first considering and rejecting the government's classified state
17 secrets submission.

18 Plaintiffs nonetheless contend that the existence of any such certifications "cannot
19 be immunized from disclosure on the ground of the 'state secrets privilege.'" Pltfs. Mem. at
20 8. That is so, they claim, because "[d]iscovery of such certifications . . . is *required* by"
21 section 2511(2)(a)(ii). *Id.* at 14 (emphasis added). Both the premise and the conclusion are
22 wrong. Section 2511(2)(a)(ii) does not require discovery of anything. To the contrary, it
23 *forbids* providers from disclosing any such certifications "except as may otherwise be
24 required by legal process." 18 U.S.C. § 2511(2)(a)(ii).

25

26

27 ⁸ The Court is, however, free to resolve these issues based on the fatal defects in plaintiffs'
28 pleadings, as we have contended it should in our motion to dismiss.

28

1 But even if § 2511(2)(a)(ii) did generally require or authorize discovery of
2 certifications, that could not overcome the Executive's constitutionally-based privilege to
3 protect from disclosure information about the existence or non-existence of *particular*
4 certifications where it is necessary to protect military or state secrets – as the Ninth Circuit
5 squarely held in *Kasza v. Browner*, 133 F.3d 1159, 1167-68 (9th Cir. 1998). In *Kasza*, the
6 plaintiffs contended that a federal statute narrowly codified the scope of the President's
7 privilege to exempt federal facilities from environmental information disclosure
8 requirements and that no broader exemption could be asserted under the state secrets
9 privilege. The Court rejected that argument, equating it to an assertion that Congress had
10 "preempted" the President's federal common law state secrets privilege. *Id.* at 1167. The
11 Court explained that any such argument must necessarily fail unless "the statute speaks
12 directly to the question otherwise answered by the common law," *id.* (*quoting County of*
13 *Oneida v. Oneida Indian Nation*, 470 U.S. 226, 236-37 (1985)), and it cautioned that
14 statutes "are to be read with a presumption favoring the retention of long-established and
15 familiar principles, except when a contrary statutory purpose to the contrary is evident." *Id.*
16 at 1167 (*quoting United States v. Texas*, 507 U.S. 529, 434 (1993)). The Court then
17 rejected the preemption claim, finding "no Congressional intent to replace the government's
18 evidentiary privilege to withhold sensitive information in litigation by providing" a
19 statutory exemption. *Id.* at 1168 ("At times the purposes of the privilege and the exemption
20 may overlap, but that does not mean that [the statute] 'speaks directly' to the existence, or
21 exercise, of the privilege in every RCRA action", "if a facility hasn't been exempted . . . it
22 might still be the case that disclosure of discrete items of relevant information would affect
23 the national interest").

24 The same conclusion is compelled here. Nothing in section 2511(2)(a)(ii) remotely
25 suggests that Congress intended to deprive the Executive Branch of the ability to assert its
26 privilege to deny discovery that would risk harm to national security – even assuming that
27 Congress could do so consistent with core constitutional separation of powers principles.

28

1 See, e.g., *Frost v. Perry*, 161 F.R.D. 434, 439 (D. Nev. 1995) (“the Court finds it
2 implausible that Congress, without ‘more explicit statutory language and legislative
3 comment,’ intended to preempt or supersede a common law privilege with constitutional
4 underpinnings) (*quoting Fogerty v. Fantasy, Inc.*, 510 U.s. 517, 534 (1994)). Indeed, §
5 2511 evinces precisely the opposite intent: its principal thrust is to *forbid* any disclosure of
6 a certification until after the Attorney General has been notified and thereby given an
7 opportunity to interpose the kinds of privileges or objections he has asserted in this case. In
8 other words, the statute is, on its face, designed to *preserve* the very privilege the plaintiffs
9 claim it overrides. See H.R. Rep. No. 95-1283, at 99 n.53 (1978) (“The notice provision is
10 intended to provide sufficient time for the Government to intervene to quash a subpoena or
11 otherwise take legal action to prevent disclosure if it so desires.”).

12 Here, of course, the government already has exercised its discretion to invoke the
13 state secrets privilege to deny discovery of any information that would confirm or deny
14 AT&T’s participation in the alleged government intelligence activities or any certifications
15 or other authorizations that AT&T may or may not have received. The Court accordingly
16 cannot adjudicate the question whether AT&T has section 2511(2)(a)(ii) immunity from
17 plaintiffs’ claims or allow discovery of the existence or non-existence of any certifications
18 AT&T may have received without reviewing the government’s classified state secrets
19 showing. Because plaintiffs acknowledge that the existence of a certification could provide
20 AT&T with complete immunity from suit or, alternatively, a good-faith defense to all their
21 claims, it is apparent that, for this reason alone, plaintiffs’ claim that they “can make their
22 case based on the public record,” Pltfs. Mem. at 5, is flat wrong.

23 In all events, AT&T has numerous other legal and factual defenses that would be
24 implicated by litigation of this case, regardless of whether or not certifications exist. To
25 take just one example already cited in AT&T’s motion to dismiss, even if one assumes that
26 AT&T participated in the terrorist surveillance program as alleged and that it did not enjoy
27 statutory immunity, AT&T would still be entitled to assert the common law immunities

28

1 from suit that are available to telecommunications carriers who are alleged to be
2 cooperating with surveillance activities that the government has assured the carrier are
3 lawful. *See, e.g., Smith v. Nixon*, 606 F.2d 1183, 1191 (D.C. Cir. 1979); *Halperin v.*
4 *Kissinger*, 424 F. Supp. 838, 846 (D.D.C. 1976), *rev'd on other grounds*, 606 F.2d 1192
5 (D.C. Cir. 1979). Consideration of absolute or qualified common law immunity, to the
6 extent they did not provide a basis for dismissal on the pleadings, would entail detailed
7 consideration of the facts and circumstances of the carrier's cooperation, including the
8 representations made to the carrier, what specific actions were taken by the carrier's
9 employees, what role the carrier had in the surveillance, and what, if any, use was made of
10 any data. All of this is within the scope of the United States' existing claim of privilege,
11 and evaluation of these issues could not possibly occur without first confronting that claim.

12 * * * *

13 The appropriate way to resolve the state secrets issue in this case is the normal and
14 accepted way: this Court should review the classified submission of the United States,
15 decide whether it satisfies the legal criteria for invoking the state secrets privilege and
16 supports the government's request for dismissal of this case, and rule accordingly. There is
17 no reason to deviate from this established procedure or to accept plaintiffs' invitation to
18 engage in legal contortions in an attempt to avoid confronting the threshold question on
19 which most other questions in this case depend. Until that question is resolved, no
20 discovery of information covered by the government's assertion of privilege, including the
21 existence *vel non* of certifications, should be ordered.
22

23
24
25
26
27
28

1 **III. CONCLUSION.**

2 For the foregoing reasons, the Court should adhere to its current plan and review the
3 government's classified submissions prior to argument on the pending motions to dismiss
4 on June 23, 2006. No discovery should be ordered unless and until those motions are
5 denied.

6
7 Dated: May 24, 2006.

8
9 PILLSBURY WINTHROP
10 SHAW PITTMAN LLP
11 BRUCE A. ERICSON
12 DAVID L. ANDERSON
13 JACOB R. SORENSEN
14 BRIAN J. WONG
15 50 Fremont Street
16 Post Office Box 7880
17 San Francisco, CA 94120-7880

SIDLEY AUSTIN LLP
DAVID W. CARPENTER
DAVID L. LAWSON
BRADFORD A. BERENSON
EDWARD R. MCNICHOLAS
1501 K Street, N.W.
Washington, D.C. 20005

18
19 By /s/ Bruce A. Ericson
20 Bruce A. Ericson

By /s/ Bradford A. Berenson
Bradford A. Berenson

21
22 *Attorneys for Defendants AT&T CORP. and AT&T INC.*
23
24
25
26
27
28

EXHIBIT I

1 Plaintiffs' principal argument is that the court need not
2 address the state secrets issue nor review the classified documents
3 because plaintiffs can make their *prima facie* case based solely on
4 the public record, including government admissions regarding the
5 wiretapping program and non-classified documents provided by former
6 AT&T technician Mark Klein. Doc #134 (Pl Redact Br) at 5-8. Even
7 if plaintiffs are correct in this argument, it does not afford
8 sufficient reason to delay deciding the state secrets issue.

9 The government asserts that "the very subject matter of
10 Plaintiffs' allegations is a state secret and further litigation
11 would inevitably risk their disclosure." Doc #145-1 (Gov Br) at
12 14. If the government is correct, then "the court should dismiss
13 [plaintiffs'] action based solely on the invocation of the state
14 secrets privilege." Kasza v Browner, 133 F3d 1159, 1166 (9th Cir
15 1998). Moreover, until the applicability and reach of the
16 privilege is ascertained, AT&T might be prevented from using
17 certain crucial evidence, such as whether AT&T received a
18 certification from the government. See Gov Br at 16-17. See also
19 Kasza, 133 F3d at 1166 (noting that a defendant might be entitled
20 to summary judgment if "the privilege deprives the defendant of
21 information that would otherwise give the defendant a valid defense
22 to the claim" (quoting Bareford v General Dynamics Corp, 973 F2d
23 1138, 1141 (5th Cir 1992)) (emphasis and internal quotation marks
24 omitted)). The state secrets issue might resolve the case,
25 discovery or further motion practice might inadvertently cause
26 state secrets to be revealed and AT&T's defense might be hindered
27 until the scope of the privilege is clarified. Hence, the court
28 agrees with the government that the state secrets issue should be

1 addressed first.

2 To address this issue, the government claims that the
3 court should examine the classified documents, which apparently
4 "disclose the sources and methods, the intelligence activities,
5 etc, that could be brought into play by the allegations in
6 plaintiffs' complaint." Doc #138 (5/17/06 Transcript) at 34:15-17.
7 Because the government contends that "the primary reasons for
8 rejecting Plaintiffs' arguments are set forth in the Government's
9 *in camera, ex parte* materials," Gov Br at 13, the court would be
10 remiss not to consider those classified documents in determining
11 whether this action is barred by the privilege. And although the
12 court agrees with plaintiffs that it must determine the scope of
13 the privilege before ascertaining whether this case implicates
14 state secrets, Pl Redact Br at 13-14, review of the classified
15 documents is necessary to determine the privilege's scope.

16 Plaintiffs also contend that "the government must make a
17 more specific showing [in its public filings] than it has before
18 this Court may be required to review secret filings *ex parte*." Id
19 at 10. But the government, via Director of National Intelligence
20 John D Negroponete, has stated that "any further elaboration on the
21 public record concerning these matters would reveal information
22 that could cause the very harms my assertion of the state secrets
23 privilege is intended to prevent." Doc #124-2 (Negroponete Decl), ¶
24 12. See also Doc #124-3 (Alexander Decl), ¶ 8. Although the court
25 may later require the government to provide a more specific public
26 explanation why the state secrets privilege must be invoked,
27 Ellsberg v Mitchell, 709 F2d 51, 63-64 (DC Cir 1983), the court
28 cannot, without first examining the classified documents, determine

1 whether the government could provide a more detailed public
2 explanation without potentially "forc[ing] 'disclosure of the very
3 thing the privilege is designed to protect.'" Id at 63 (quoting
4 United States v Reynolds, 345 US 1, 8 (1953)).

5 Plaintiffs further assert that adjudicating whether AT&T
6 received any certification does not require the court to review the
7 classified documents. Specifically, plaintiffs rely on 18 USC §
8 2511(2)(a)(ii)(B), which states in relevant part (emphasis added):

9 No provider of wire or electronic communication service
10 * * * or other specified person shall disclose the
11 existence of any interception or surveillance or the
12 device used to accomplish the interception or
13 surveillance with respect to which the person has been
14 furnished an order or certification under this
subparagraph, except as may otherwise be required by
legal process and then only after prior notification to
the Attorney General or to the principal prosecuting
attorney of a State or any political subdivision of a
State, as may be appropriate.

15 Plaintiffs claim that the phrase "except as may otherwise be
16 required by legal process" means that "if the AT&T defendants are
17 claiming that they have a certification defense, then 'legal
18 process' would require the disclosure of the fact of that
19 certification in the ordinary course of litigation." Pl Redact Br
20 at 8-9.

21 This argument fails, however, because the government's
22 "state secrets assertion 'covers any information tending to confirm
23 or deny' whether 'AT&T was involved with any' of the 'alleged
24 intelligence activities.'" Gov Br at 17 (quoting Doc #124-1 (Gov
25 Mot Dis) at 17-18). Because the existence or non-existence of a
26 certification would tend to prove or disprove whether AT&T was
27 involved in the alleged intelligence activities, the privilege as
28 claimed prevents the disclosure of any certification. And because

1 the "legal process" could not require AT&T to disclose a
2 certification if the state secrets privilege prevented such
3 disclosure, discovery on the certification issue cannot proceed
4 unless the court determines that the privilege does not apply with
5 respect to that issue.

6 Finally, plaintiffs claim that they should be able to
7 review the classified documents alongside the court. Plaintiffs
8 note that due process disfavors deciding this case based on secret
9 evidence and they contend that "the Court should proceed
10 incrementally, examining only the least amount of *ex parte*
11 information when – and if – this becomes absolutely necessary." Pl
12 Redact Br at 3. Although *ex parte*, *in camera* review is
13 extraordinary, this form of review is the norm when state secrets
14 are at issue. See Kasza, 133 F3d at 1169 ("Elaborating the basis
15 for the claim of privilege through *in camera* submissions is
16 unexceptionable."). See also Black v United States, 62 F3d 1115,
17 1119 & n6 (8th Cir 1995); Ellsberg, 709 F2d at 60 ("It is well
18 settled that a trial judge called upon to assess the legitimacy of
19 a state secrets privilege claim should not permit the requester's
20 counsel to participate in an *in camera* examination of putatively
21 privileged material."). And for the reasons stated above, review
22 of the classified documents is necessary here to determine whether
23 the state secrets privilege applies.

24 Plaintiffs also contend that a statutory provision, 50
25 USC § 1806(f), entitles them to review the classified documents.
26 Pl Redact Br at 4. Section 1806(f) provides in relevant part:

27 //

28 //

United States District Court
For the Northern District of California

1 [W]henever any motion or request is made by an aggrieved
2 person * * * to discover or obtain applications or orders
3 or other materials relating to electronic surveillance
4 * * * the United States district court * * * shall,
5 notwithstanding any other law, if the Attorney General
6 files an affidavit under oath that disclosure or an
7 adversary hearing would harm the national security of the
8 United States, review *in camera* and *ex parte* the
9 application, order, and such other materials relating to
10 the surveillance as may be necessary to determine whether
11 the surveillance of the aggrieved person was lawfully
12 authorized and conducted. In making this determination,
13 the court may disclose to the aggrieved person, under
14 appropriate security procedures and protective orders,
15 portions of the application, order, or other materials
16 relating to the surveillance only where such disclosure
17 is necessary to make an accurate determination of the
18 legality of the surveillance.

11 Plaintiffs contend if the court determines that it must review the
12 classified documents, this provision indicates that the court
13 "should do so under conditions that provide for some form of
14 appropriate access by plaintiffs' counsel." Pl Redact Br at 4.

15 The government and AT&T contend that this provision is
16 inapplicable here because "[p]laintiffs' claims are based on their
17 contention that the alleged surveillance activities should have
18 occurred under FISA, but allegedly did not, whereas the review
19 available under section 1806(f) is available only when electronic
20 surveillance did, in fact, occur 'under this chapter.'" Gov Br at
21 11 (citation omitted); Doc #150 (AT&T Redact Br) at 10. Even if
22 this provision applies to the present case, it does not follow that
23 plaintiffs are entitled to view some or all of the classified
24 documents at this time. Section 1806(f) requires the court to
25 "review *in camera* and *ex parte* the application, order, and such
26 other materials relating to the surveillance" when determining
27 whether the surveillance was legal. Only after such review may the
28 court disclose the protected materials to the aggrieved person to

1 the extent "necessary to make an accurate determination of the
2 legality of the surveillance." Hence, § 1806(f) does not provide
3 plaintiffs with a present right to view the classified documents.

4 The court is mindful of the extraordinary due process
5 consequences of applying the privilege the government here asserts.
6 The court is also mindful of the government's claim of
7 "exceptionally grave damage to the national security of the United
8 States" (Negroponte Decl, ¶ 3) that failure to apply the privilege
9 could cause. At this point, review of the classified documents
10 affords the only prudent way to balance these important interests.

11 Accordingly, because review of the classified documents
12 is necessary to determine whether and to what extent the state
13 secrets privilege applies, the court ORDERS the government
14 forthwith to provide *in camera* and no later than June 9, 2006, the
15 classified memorandum and classified declarations of John D
16 Negroponte and Keith B Alexander for review by the undersigned and
17 by any chambers personnel that he so authorizes.

18
19 IT IS SO ORDERED.

20 
21 _____

22 VAUGHN R WALKER
23 United States District Chief Judge
24
25
26
27
28

United States District Court
For the Northern District of California

EXHIBIT J



OFFICE OF
THE CHAIRMAN

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

May 22, 2006

The Honorable Edward J. Markey
Ranking Member
Subcommittee on Telecommunications and the Internet
Energy and Commerce Committee
U.S. House of Representatives
2108 Rayburn House Office Building
Washington, D.C. 20515

Dear Congressman Markey:

Thank you for your letter regarding recent media reports concerning the collection of telephone records by the National Security Agency. In your letter, you note that section 222 of the Communications Act provides that "[e]very telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to . . . customers." 47 U.S.C. § 222(a). You have asked me to explain the Commission's plan "for investigating and resolving these alleged violations of consumer privacy."

I know that all of the members of this Commission take very seriously our charge to faithfully implement the nation's laws, including our authority to investigate potential violations of the Communications Act. In this case, however, the classified nature of the NSA's activities makes us unable to investigate the alleged violations discussed in your letter at this time.

The activities mentioned in your letter are currently the subject of an action filed in the United States District Court for the Northern District of California. The plaintiffs in that case allege that the NSA has "arrang[ed] with some of the nation's largest telecommunications companies . . . to gain direct access to . . . those companies' records pertaining to the communications they transmit." *Hepting v. AT&T Corp.*, No. C-06-0672-VRW (N.D. Cal.), Amended Complaint ¶ 41 (Feb. 22, 2006). According to the complaint, for example, AT&T Corp. has provided the government "with direct access to the contents" of databases containing "personally identifiable customary proprietary network information (CPNI)," including "records of nearly every telephone communication carried over its domestic network since approximately 2001, records that include the originating and terminating telephone numbers and the time and length for each call." *Id.* ¶¶ 55, 56, 61; *see also, e.g.*, Leslie Cauley, "NSA Has Massive Database of Americans' Phone Calls," *USA Today* A1 (May 11, 2006) (alleging that the NSA "has been secretly collecting the phone call records of tens of millions of Americans, using data provided" by major telecommunications carriers).

The government has moved to dismiss the action on the basis of the military and state secrets privilege. See *Hepting*, Motion to Dismiss or, in the Alternative, for Summary Judgment by the United States of America (May 12, 2006). Its motion is accompanied by declarations from John D. Negroponete, Director of National Intelligence, and Lieutenant General Keith B. Alexander, Director, National Security Agency, who have maintained that disclosure of information “implicated by Plaintiffs’ claims . . . could reasonably be expected to cause exceptionally grave damage to the national security of the United States.” Negroponete Decl. ¶ 9. They specifically address “the NSA’s purported involvement” with specific telephone companies, noting that “the United States can neither confirm nor deny alleged NSA activities, relationships, or targets,” because “[t]o do otherwise when challenged in litigation would result in the exposure of intelligence information, sources, and methods and would severely undermine surveillance activities in general.” Alexander Decl. ¶ 8.

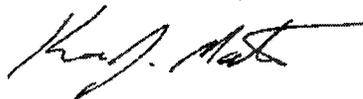
The representations of Director Negroponete and General Alexander make clear that it would not be possible for us to investigate the activities addressed in your letter without examining highly sensitive classified information. The Commission has no power to order the production of classified information. Rather, the Supreme Court has held that “the protection of classified information must be committed to the broad discretion of the agency responsible, and this must include broad discretion to determine who may have access to it. Certainly, it is not reasonably possible for an outside nonexpert body to review the substance of such a judgment.” *Department of the Navy v. Egan*, 484 U.S. 518, 529 (1988).

The statutory privilege applicable to NSA activities also effectively prohibits any investigation by the Commission. The National Security Act of 1959 provides that “nothing in this Act or any other law . . . shall be construed to require the disclosure of the organization or any function of the National Security Agency [or] of any information with respect to the activities thereof.” Pub. L. No. 86-36, § 6(a), 73 Stat. 63, 64, codified at 50 U.S.C. § 402 note. As the United States Court of Appeals for the District of Columbia Circuit has explained, the statute’s “explicit reference to ‘any other law’ . . . must be construed to prohibit the disclosure of information relating to NSA’s functions and activities as well as its personnel.” *Linder v. NSA*, 94 F.3d 693, 696 (D.C. Cir. 1996); see also *Hayden v. NSA/Central Sec. Serv.*, 608 F.2d 1381, 1390 (D.C. Cir. 1979) (“Congress has already, in enacting the statute, decided that disclosure of NSA activities is potentially harmful.”). This statute displaces any authority that the Commission might otherwise have to compel, at this time, the production of information relating to the activities discussed in your letter.

Page 3—The Honorable Edward J. Markey

I appreciate your interest in this important matter. Please do not hesitate to contact me if you have further questions.

Sincerely,

A handwritten signature in black ink, appearing to read "Kevin J. Martin". The signature is fluid and cursive, with a long horizontal stroke extending to the right.

Kevin J. Martin
Chairman

EXHIBIT K

PETER D. KEISLER
 Assistant Attorney General
 CHRISTOPHER J. CHRISTIE
 United States Attorney
 SUSAN STEELE
 Assistant United States Attorney
 CARL J. NICHOLS
 Deputy Assistant Attorney General
 DOUGLAS LETTER
 Terrorism Litigation Counsel
 ARTHUR R. GOLDBERG
 Assistant Director, Federal Programs Branch
 ALEXANDER HAAS
 Trial Attorney, Federal Programs Branch
 UNITED STATES DEPARTMENT OF JUSTICE
 P.O. BOX 883
 WASHINGTON, DC 20044
 (202) 307-3937

BY: IRENE DOWDY
 Assistant United States Attorney
 (609) 989-0562

UNITED STATES DISTRICT COURT
 FOR THE DISTRICT OF NEW JERSEY

THE UNITED STATES OF AMERICA,)
)
 Plaintiff,)
)
 v.)
)
 ZULIMA V. FARBER, in her official capacity as)
 Attorney General of the State of New Jersey;)
 CATHLEEN O'DONNELL, in her official)
 capacity as Deputy Attorney General of the State)
 of New Jersey; KIMBERLY S. RICKETTS, in)
 her official capacity as Director of the New Jersey)
 Division of Consumer Affairs; AT&T CORP.;)
 VERIZON COMMUNICATIONS INC; QWEST)
 COMMUNICATIONS INTERNATIONAL, INC.;)
 SPRINT NEXTEL CORPORATION; and)
 CINGULAR WIRELESS LLC,)
)
 Defendants.)

CIVIL ACTION NO.:
 COMPLAINT

Plaintiff, the United States of America, by its undersigned attorneys, brings this civil action for declaratory and injunctive relief, and alleges as follows:

INTRODUCTION

1. In this action, the United States seeks to prevent the disclosure of highly confidential and sensitive government information that the defendant officers of the State of New Jersey have sought to obtain from telecommunications carriers without proper authorization from the United States. Compliance with the subpoenas issued by those officers would first place the carriers in a position of having to confirm or deny the existence of information that cannot be confirmed or denied without causing exceptionally grave harm to national security. And if particular carriers are indeed supplying foreign intelligence information to the Federal Government, compliance with the subpoenas would require disclosure of the details of that activity. The defendant state officers' attempts to obtain such information are invalid under the Supremacy Clause of the United States Constitution and are preempted by the United States Constitution and various federal statutes. This Court should therefore enter a declaratory judgment that the State Defendants do not have the authority to seek confidential and sensitive federal government information and thus cannot enforce the subpoenas they have served on the telecommunications carriers.

JURISDICTION AND VENUE

2. The Court has jurisdiction pursuant to 28 U.S.C. §§ 1331, 1345.
3. Venue lies in the District of New Jersey pursuant to 28 U.S.C. § 1391(b)(1) and (2).

PARTIES

4. Plaintiff is the United States of America, suing on its own behalf.
5. Defendant Zulima V. Farber is the Attorney General for the State of New Jersey, and maintains her offices in Mercer County. She is being sued in her official capacity.
6. Defendant Cathleen O'Donnell is the Deputy Attorney General for the State of New Jersey, and maintains her offices in Mercer County. She is being sued in her official capacity.
7. Defendant Kimberly S. Ricketts is the Director of the New Jersey Division of Consumer Affairs. She is being sued in her official capacity. Defendants Zulima V. Farber, Cathleen O'Donnell, and Kimberly S. Ricketts are referred to as the "State Defendants."
8. Defendant AT&T Corp. is a corporation incorporated in the state of New York with its principal place of business in Somerset County, New Jersey, and that has received a subpoena in New Jersey.
9. Defendant Verizon Communications Inc. is a corporation incorporated in the state of Delaware with its principal place of business in the state of New York, that has offices in Somerset County, New Jersey, and that has received a subpoena in New Jersey.
10. Defendant Qwest Communications International, Inc. is a corporation incorporated in the state of Delaware with its principal place of business in the state of Colorado, and that has received a subpoena in New Jersey.
11. Defendant Sprint Nextel Corporation is a corporation incorporated in the state of New Jersey with its principal place of business in the state of Virginia, and that has received a subpoena in New Jersey.
12. Defendant Cingular Wireless LLC is a corporation incorporated in the state of Delaware with its principal place of business in Georgia, and that has received a subpoena in

New Jersey.

13. Defendants AT&T Corp., Cingular Wireless LLC, Qwest Communications International, Inc., Sprint Nextel Corporation, and Verizon Communications, Inc. are referred to as the "Carrier Defendants."

STATEMENT OF THE CLAIM

I. The Federal Government Has Exclusive Control Vis-a-Vis the States With Respect to Foreign-Intelligence Gathering, National Security, the Conduct of Foreign Affairs, and the Conduct of Military Affairs.

14. The Federal Government has exclusive control vis-a-vis the States over foreign-intelligence gathering, over national security, and over the conduct of war with foreign entities. The Federal Government controls the conduct of foreign affairs, the conduct of military affairs, and the performance of the country's national security function.

15. In addition, various federal statutes and Executive Orders govern and regulate access to information relating to foreign intelligence gathering.

16. For example, Section 102A(i)(1) of the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638 (Dec. 17, 2004), codified at 50 U.S.C. § 403-1(i)(1), confers upon the Director of National Intelligence the authority and responsibility to "protect intelligence sources and methods from unauthorized disclosure."

17. Federal law also makes it a felony for any person to divulge classified information "concerning the communication intelligence activities of the United States" to any person who has not been authorized by the President, or his lawful designee, to receive such information. 18 U.S.C. § 798.

18. And federal law establishes unique protections from disclosure for information related to the National Security Agency. Federal law states that "nothing in this . . . or any other

law . . . shall be construed to require disclosure of . . . any function of the National Security Agency, [or] of any information with respect to the activities thereof." 50 U.S.C. § 402 note.

19. Several Executive Orders have been promulgated pursuant to these constitutional and statutory authorities that govern access to and handling of national security information.

20. First, Executive Order No. 12958, 60 Fed. Reg. 19825 (April 17, 1995), as amended by Executive Order No. 13292, 68 Fed. Reg. 15315 (March 25, 2003), prescribes a uniform system for classifying, safeguarding and declassifying national security information. It provides that:

A person may have access to classified information provided that:

- (1) a favorable determination of eligibility for access has been made by an agency head or the agency head's designee;
- (2) the person has signed an approved nondisclosure agreement; and
- (3) the person has a need-to-know the information.

Exec. Order No. 13292, Sec. 4.1(a). "Need-to-know" means "a determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function." Exec. Order No. 12958, Sec. 4.1(c). Executive Order No. 12958 further states, in part, that "Classified information shall remain under the control of the originating agency or its successor in function." Exec. Order No. 13292, Sec. 4.1(c).

21. Second, Executive Order No. 12968, 60 Fed. Reg. 40245 (Aug. 2, 1995), establishes a uniform Federal personnel security program for employees of the Federal Government, as well as employees of an industrial or commercial contractor of a Federal agency, who will be considered for initial or continued access to the classified information. The Order states, in part,

that "Employees who are granted eligibility for access to classified information shall . . . protect classified information in their custody from unauthorized disclosure . . ." Exec. Order No. 12968, Sec. 6.2(a)(1).

22. In addition, the courts have developed several doctrines that are relevant to this dispute and that establish the supremacy of federal law with respect to national security information and intelligence gathering. For example, suits alleging secret espionage agreements with the United States are not justiciable.

23. The Federal Government also has an absolute privilege to protect military and state secrets from disclosure. Only the Federal Government can waive that privilege, which is often called the "state secrets privilege."

II. The Terrorist Surveillance Program and the Federal Government's Invocation of the State Secrets Privilege

24. The President has explained that, following the devastating events of September 11, 2001, he authorized the National Security Agency ("NSA") to intercept certain international communications into and out of the United States of persons linked to al Qaeda or related terrorist organizations. See Press Conference of President Bush (Dec. 19, 2005), available at <http://www.whitehouse.gov/news/releases/2005/12/20051219-2.html>. ("President's Press Release").

25. The Attorney General of the United States has further explained that, in order to intercept a communication, there must be "a reasonable basis to conclude that one party to the communication is a member of al Qaeda, affiliated with al Qaeda, or a member of an organization affiliated with al Qaeda." Press Briefing by Attorney General Alberto Gonzales and General Michael Hayden, Principal Deputy Director for National Intelligence (Dec. 19, 2005),

available at <http://whitehouse.gov/news/releases/2005/12/20051219-1.html>. This activity is known as the Terrorist Surveillance Program ("TSP").

26. The purpose of these intercepts is to provide the United States with an early warning system to detect and prevent another catastrophic terrorist attack in the United States. See President's Press Release. The President has stated that the NSA activities "ha[ve] been effective in disrupting the enemy, while safeguarding our civil liberties." *Id.*

27. Since January 2006, more than 20 class action lawsuits have been filed alleging that telecommunications carriers, including the Carrier Defendants, have unlawfully provided assistance to the NSA. The first lawsuit, *Hepting v. AT&T Corp., et al.*, was filed in the District Court for the Northern District of California in January 2006. Case No. C-06-0672-VRW.

28. Those lawsuits, including the *Hepting* case, generally make two sets of allegations. First, the lawsuits allege that the telecommunications carriers unlawfully intercepted the contents of certain telephone calls and emails and provided them to the NSA. Second, the lawsuits allege that telecommunications carriers have unlawfully provided the NSA with access to calling records and related information.

29. The Judicial Panel on Multidistrict Litigation is currently considering a motion to transfer all of these lawsuits to a single district court for pretrial proceedings. *In re: National Security Agency Telecommunications Records Litigation*, MDL Docket No. 1791 (JPML).

30. In the *Hepting* case, the state secrets privilege has been formally asserted by the Director of National Intelligence, John D. Negroponte, and the Director of the National Security Agency, Lieutenant General Keith B. Alexander. The Director of National Intelligence is the "head of the intelligence community" of the United States. 50 U.S.C. § 403(b)(1). General Alexander has also invoked the NSA's statutory privilege. See 50 U.S.C. § 402 note.

31. The public declarations of the Director of National Intelligence and the Director of the NSA in the *Hepting* case state that, “[i]n an effort to counter the al Qaeda threat, the President of the United States authorized the NSA to utilize its [signals intelligence] capabilities to collect certain ‘one-end foreign’ communications where one party is associated with the al Qaeda terrorist organization for the purpose of detecting and preventing another terrorist attack on the United States. This activity is known as the Terrorist Surveillance Program (‘TSP’).” Negroponete Decl. ¶ 11 (Exhibit A, attached to this Complaint); see Alexander Decl. ¶ 7 (Exhibit B, attached to this Complaint).

32. Director Negroponete and General Alexander have concluded that “[t]o discuss this activity in any greater detail, however, would disclose classified intelligence information and reveal intelligence sources and methods, which would enable adversaries of the United States to avoid detection by the U.S. Intelligence Community and/or take measures to defeat or neutralize U.S. intelligence collection, posing a serious threat of damage to the United States’ national security interests.” Negroponete Decl. ¶ 11; see Alexander Decl. ¶ 7.

33. The public declarations further state that “any further elaboration on the public record concerning these matters would reveal information that could cause the very harms [that] the assertion of the state secrets privilege is intended to prevent.” Negroponete Decl. ¶ 12; see Alexander Decl. ¶ 8. The assertion of the privilege encompasses “allegations about NSA’s purported involvement with AT&T.” Negroponete Decl. ¶ 12; Alexander Decl. ¶ 8. Director Negroponete and General Alexander have explained that “[t]he only recourse for the Intelligence Community and, in this case, for the NSA, is to neither confirm nor deny these sorts of allegations, regardless of whether they are true or false. To say otherwise when challenged in

litigation would result in routine exposure of intelligence information, sources, and methods and would severely undermine surveillance activities in general." Negroponte Decl. ¶ 12; see Alexander Decl. ¶ 8.

III. The State Defendants Seek to Require the Production of Potentially Highly Classified and Sensitive Information

34. On May 17, 2006, the State Defendants sent subpoenas duces tecum entitled "Provision of Telephone Call History Data to the National Security Agency" ("Subpoenas") to each of the Carrier Defendants. A representative Subpoena is attached as Exhibit C. The materials sought by these Subpoenas include, among other items, "[a]ll names and complete addresses of Persons including, but not limited to, all affiliates, subsidiaries and entities, that provide Telephone Call History Data to the NSA";¹ "[a]ll Executive Orders issued by the President of the United States and provided to Verizon concerning any demand or request to provide Telephone Call History Data to the NSA"; "[a]ll orders, subpoenas and warrants issued by or on behalf of any unit or officer of the Executive Branch of the Federal Government and provided to Verizon concerning any demand or request to provide Telephone Call History Data to the NSA"; "[a]ll orders, subpoenas and warrants issued by or on behalf of any Federal or State judicial authority and provided to Verizon concerning any demand or request to provide Telephone Call History Data to the NSA"; "[a]ll Documents concerning the basis for Verizon's provision of Telephone Call History Data to the NSA, including, but not limited to, any legal or contractual authority"; "[a]ll Documents concerning any written or oral contracts, memoranda of

¹ Under the Subpoenas, "'Telephone Call History Data' means any data Verizon provided to the NSA including, but not limited to, records of landline and cellular telephone calls placed, and/or received by a Verizon subscriber with a New Jersey billing address or New Jersey telephone number." See Definitions, ¶ 8.

understanding, memoranda of agreement, other agreements or correspondence by or on behalf of Verizon and the NSA concerning the provision of Telephone Call History Data to the NSA"; "[a]ll Documents concerning any communication between Verizon and the NSA or any other unit or officer of the Executive Branch of the Federal Government concerning the provision of Telephone Call History Data to the NSA"; and "[t]o the extent not otherwise requested, [a]ll Documents concerning any demand or request that Verizon provide Telephone Call History Data to the NSA." See Subpoenas, ¶¶ 1-13.

35. These Subpoenas specify that they are "issued pursuant to the authority of N.J.S.A. 56:8-1, et seq., specifically N.J.S.A. 56:8-3 and 56:8-4." The cited provisions of state law concern consumer fraud, and provide, *inter alia*, that "[w]hen it shall appear to the [state] Attorney General that a person has engaged in, is engaging in, or is about to engage in any practice declared to be unlawful by this act, or when he believes it to be in the public interest that an investigation should be made to ascertain whether a person in fact has engaged in, is engaging in or is about to engage in, any such practice, he may . . . [e]xamine any merchandise or sample thereof, record, book, document, account or paper as he may deem necessary." N.J.S.A. 56:8-3. "To accomplish the objectives and to carry out the duties prescribed by this act, the [state] Attorney General, in addition to other powers conferred upon him by this act, may issue subpoenas to any person, administer an oath or affirmation to any person, conduct hearings in aid of any investigation or inquiry, promulgate such rules and regulations, and prescribe such forms as may be necessary, which shall have the force of law." N.J.S.A. 56:8-4.

36. The cover letter accompanying these Subpoenas states: "Failure to comply with this Subpoena may render you liable for contempt of court and such other penalties as are provided

by law.”

37. These Subpoenas demand that responses be submitted by the Carrier Defendants on or before May 30, 2006. The State Defendants have extended the time for responses to June 15, 2006.

IV. The State Defendants Lack Authority to Compel Compliance with the Subpoenas.

38. The State Defendants’ authority to seek or obtain the information requested in these Subpoenas is fundamentally inconsistent with and preempted by the Federal Government’s exclusive control over all foreign intelligence gathering activities. In addition, no federal law authorizes the State Defendants to obtain the information they seek.

39. The State Defendants have not been granted access to classified information related to the activities of the NSA pursuant to the requirements set out in Executive Order No. 12958 or Executive Order No. 13292.

40. The State Defendants have not been authorized to receive classified information concerning the communication intelligence activities of the United States in accordance with the terms of 18 U.S.C. § 798, or any other federal law, regulation, or order.

41. In seeking information bearing upon NSA’s purported involvement with the Carrier Defendants, the Subpoenas seek disclosure of matters with respect to which the Director of National Intelligence has determined that disclosure, including confirming or denying whether or to what extent such materials exist, would improperly reveal intelligence sources and methods.

42. The United States has a strong and compelling interest in preventing the disclosure of sensitive and classified information. The United States has a strong and compelling interest in preventing terrorists from learning about the methods and operations of terrorist surveillance

activities being undertaken or not being undertaken by the United States.

43. As a result of the Constitution, federal laws, applicable privileges, and the United States' interest in preventing the unauthorized disclosure of sensitive or classified information, the Carrier Defendants will be unable to confirm or deny their involvement, if any, in intelligence activities of the United States, and therefore cannot provide a substantive response to the Subpoenas.

44. The United States will be irreparably harmed if the Carrier Defendants are permitted or are required to disclose sensitive and classified information to the State Defendants in response to the Subpoenas.

**COUNT ONE – VIOLATION OF AND PREEMPTION UNDER THE SUPREMACY
CLAUSE AND FEDERAL LAW**
(ALL DEFENDANTS)

45. Plaintiff incorporates by reference paragraphs 1 through 46 above.

46. The Subpoenas, and any responses required thereto, are invalid under, and preempted by, the Supremacy Clause of the United States Constitution, Art. VI, Cl. 2, federal law, and the Federal Government's exclusive control over foreign intelligence gathering activities, national security, the conduct of foreign affairs, and the conduct of military affairs.

**COUNT TWO – UNAUTHORIZED DISCLOSURE OF SENSITIVE AND
CONFIDENTIAL INFORMATION**
(ALL DEFENDANTS)

47. Plaintiff incorporates by reference paragraphs 1 through 48 above.

48. Providing responses to the Subpoenas would be inconsistent with and would violate federal law including, but not limited to, Executive Order 12958, 18 U.S.C. § 798, and 50 U.S.C. § 402 note, as well as other applicable federal laws, regulations, and orders.

PRAYER FOR RELIEF

WHEREFORE, the United States of America prays for the following relief:

1. That this Court enter a declaratory judgment pursuant to 28 U.S.C. § 2201(a), that the Subpoenas issued by the State Defendants may not be enforced by the State Defendants or responded to by the Carrier Defendants because any attempt to obtain or disclose the information that is the subject of these Subpoenas would be invalid under, preempted by, and inconsistent with the Supremacy Clause of the United States Constitution, Art. VI, Cl. 2, federal law, and the Federal Government's exclusive control over foreign intelligence gathering activities, national security, the conduct of foreign affairs, and the conduct of military affairs.

2. That this Court grant plaintiff such other and further relief as may be just and proper, including any necessary and appropriate injunctive relief.

Respectfully submitted,

PETER D. KEISLER
Assistant Attorney General
CHRISTOPHER J. CHRISTIE
United States Attorney
SUSAN STEELE
Assistant United States Attorney
CARL J. NICHOLS
Deputy Assistant Attorney General
DOUGLAS LETTER
Terrorism Litigation Counsel
ARTHUR R. GOLDBERG
Assistant Director, Federal Programs Branch
ALEXANDER HAAS
Trial Attorney, Federal Programs Branch
U.S. DEPARTMENT OF JUSTICE
P.O. BOX 883
WASHINGTON, DC 20044
(202) 307-3937

EXHIBIT L



U. S. Department of Justice

Civil Division

Assistant Attorney General

Washington, D.C. 20530

June 14, 2006

VIA FACSIMILE AND FEDERAL EXPRESS

The Honorable Zulima V. Farber
Attorney General of New Jersey
25 Market Street
Trenton, New Jersey 08625

**Re: Subpoenas Duces Tecum Served on Telecommunications Carriers
Seeking Information Relating to the Alleged Provision of Telephone
Call History Data to the National Security Agency**

Dear Attorney General Farber:

Please find attached the Complaint filed today by the United States in the United States District Court for the District of New Jersey, in connection with the subpoenas that you have served on various telecommunications companies (the "carriers") seeking information relating to those companies' alleged provision of "telephone call history data" to the National Security Agency ("NSA"). As set forth in the Complaint, it is our belief that compliance with the subpoenas would place the carriers in a position of having to confirm or deny the existence of information that cannot be confirmed or denied without harming national security, and that enforcing compliance with these subpoenas would be inconsistent with, and preempted by, federal law.

The subpoenas infringe upon federal operations, are contrary to federal law, and accordingly are invalid under the Supremacy Clause of the United States Constitution for several reasons. The subpoenas seek to compel the disclosure of information regarding the Nation's foreign-intelligence gathering, but foreign-intelligence gathering is an exclusively federal function. Responding to the subpoenas, including disclosing whether or to what extent any responsive materials exist, would violate various specific provisions of federal statutes and Executive Orders. And the recent assertion of the state secrets privilege by the Director of National Intelligence in cases regarding the very same topics and types of information sought by your subpoenas underscores that any such information cannot be disclosed.

Although we have filed the attached Complaint at this juncture in light of the return date on the subpoenas (June 15), we nevertheless hope that this matter may be resolved amicably, and

The Honorable Zulima V. Farber
Page 2

that litigation will prove unnecessary. Toward that end, this letter outlines the basic reasons why, in our view, the state-law subpoenas are preempted by federal law. We sincerely hope that, in light of governing law and the national security concerns implicated by the subpoenas, you will withdraw them, thereby avoiding needless litigation. The United States very much appreciates your consideration of this matter.

1. There can be no question that the subpoenas interfere with and seek the disclosure of information regarding the Nation's foreign-intelligence gathering. But it has been clear since at least *McCulloch v. Maryland*, 4 U.S. 316 (1819), that state law may not regulate the Federal Government or obstruct federal operations. And foreign-intelligence gathering is an exclusively federal function; it concerns three overlapping areas that are peculiarly the province of the National Government: foreign relations and the conduct of the Nation's foreign affairs, *see American Insurance Ass'n v. Garamendi*, 539 U.S. 396, 413 (2003); the conduct of military affairs, *see Sale v. Haitian Centers Council*, 509 U.S. 155, 188 (1993) (President has "unique responsibility" for the conduct of "foreign and military affairs"); and the national security function. As the Supreme Court of the United States has stressed, there is "paramount federal authority in safeguarding national security," *Murphy v. Waterfront Comm'n of New York Harbor*, 378 U.S. 52, 76 n.16 (1964), as "[f]ew interests can be more compelling than a nation's need to ensure its own security." *Wayte v. United States*, 470 U.S. 598, 611 (1985).

The subpoenas demand that each carrier produce information regarding specified categories of communications between that carrier and the NSA since September 11, 2001, including "[a]ll names and complete addresses of Persons including, but not limited to, all affiliates, subsidiaries and entities, that provide Telephone Call History Data to the NSA";¹ any and all Executive Orders, court orders, or warrants "provided to [the carrier] concerning any demand or request to provide Telephone Call History Data to the NSA"; "[a]ll Documents concerning the basis for [the carrier's] provision of Telephone Call History Data to the NSA, including, but not limited to, any legal or contractual authority"; and "[a]ll Documents concerning any written or oral contracts, memoranda of understanding, memoranda of agreement, other agreements or correspondence by or on behalf of [the carrier] and the NSA concerning the provision of Telephone Call History Data to the NSA." *See* Document Requests, ¶¶ 1-13. In seeking to exert regulatory authority² with respect to the nation's foreign-intelligence gathering, you have thus sought to use your state regulatory authority to intrude upon a field that is reserved exclusively to the Federal Government and in a manner that interferes with federal

¹ "Telephone Call History Data" is defined as "any data [the carrier] provided to the NSA including, but not limited to, records of landline and cellular telephone calls placed, and/or received by [the carrier's] subscriber with a New Jersey billing address or New Jersey telephone number." Definitions, ¶8.

² The subpoenas make clear that they are "issued pursuant to the authority of N.J.S.A. 56:8-1 et seq., specifically N.J.S.A. 56:8-3 and 56:8-4."

The Honorable Zulima V. Farber
Page 3

prerogatives. That effort is fundamentally inconsistent with the Supremacy Clause. *McCulloch v. Maryland*, 17 U.S. (4 Wheat.) 316, 326-27, 4 L.Ed. 579 (1819) (“[T]he states have no power . . . to retard, impede, burden, or in any manner control, the operations of the constitutional laws enacted by Congress to carry into execution the power vested in the general government.”); *see also Leslie Miller, Inc. v. Arkansas*, 352 U.S. 187 (1956).

The Supreme Court’s decision in *American Insurance Ass’n v. Garamendi*, 539 U.S. 396 (2003), is the most recent precedent that demonstrates that these state-law subpoenas are preempted by federal law. In *Garamendi*, the Supreme Court held invalid subpoenas issued by the State of California to insurance carriers pursuant to a California statute that required those carriers to disclose all policies sold in Europe between 1920 and 1945, concluding that California’s effort to impose such disclosure obligations interfered with the President’s conduct of foreign affairs. Here, the subpoenas seek the disclosure of information that infringes on the Federal Government’s intelligence gathering authority and on the Federal Government’s role in protecting the national security at a time when we face terrorist threats to the United States homeland; those subpoenas, just like the subpoenas at issue in *Garamendi*, are preempted. Under the Supremacy Clause, “a state may not interfere with federal action taken pursuant to the exclusive power granted under the United States Constitution or under congressional legislation occupying the field.” *Abraham v. Hodges*, 255 F.Supp. 2d 539, 549 (D.S.C. 2002) (enjoining the state of South Carolina from interfering with the shipment of nuclear waste, a matter involving the national security, because “when the federal government acts within its own sphere or pursuant to the authority of Congress in a given field, a state may not interfere by means of conflicting attempt to promote its own local interests”).

2. Responding to the subpoenas, including merely disclosing whether or to what extent any responsive materials exist, would violate various federal statutes and Executive Orders. Section 102A(i)(1) of the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638 (Dec. 17, 2004), codified at 50 U.S.C. § 403-1(i)(1), confers upon the Director of National Intelligence (“DNI”) the authority and responsibility to “protect intelligence sources and methods from unauthorized disclosure.” *Ibid.*³ (As set forth below, the DNI has determined that disclosure of the types of information sought by the subpoenas would harm national security.) Similarly, Section 6 of the National Security Agency Act of 1959, Pub. L. No. 86-36, § 6, 73 Stat. 63, 64, codified at 50 U.S.C. § 402 note, provides: “[N]othing in this Act or

³ The authority to protect intelligence sources and methods from disclosure is rooted in the “practical necessities of modern intelligence gathering,” *Fitzgibbon v. CIA*, 911 F.2d 755, 761 (D.C. Cir. 1990), and has been described by the Supreme Court as both “sweeping,” *CIA v. Sims*, 471 U.S. 159, 169 (1985), and “wideranging.” *Snapp v. United States*, 444 U.S. 507, 509 (1980). Sources and methods constitute “the heart of all intelligence operations,” *Sims*, 471 U.S. at 167, and “[i]t is the responsibility of the [intelligence community] to weigh the variety of complex and subtle factors in determining whether disclosure of information may lead to an unacceptable risk of compromising the . . . intelligence-gathering process.” *Id.* at 180.

The Honorable Zulima V. Farber
Page 4

any other law . . . shall be construed to require the disclosure of the organization or any function of the National Security Agency, of any information with respect to the activities thereof, or of the names, titles, salaries, or number of persons employed by such agency." *Ibid.*⁴

Several Executive Orders promulgated pursuant to the foregoing constitutional and statutory authority govern access to and handling of national security information. Of particular importance here, Executive Order No. 12958, 60 Fed. Reg. 19825 (April 17, 1995), as amended by Executive Order No. 13292, 68 Fed. Reg. 15315 (March 25, 2003), prescribes a comprehensive system for classifying, safeguarding and declassifying national security information. It provides that a person may have access to classified information only where "a favorable determination of eligibility for access has been made by an agency head or the agency head's designee"; "the person has signed an approved nondisclosure agreement"; and "the person has a need-to-know the information." That Executive Order further states that "Classified information shall remain under the control of the originating agency or its successor in function." Exec. Order No. 13292, Sec. 4.1(c). Exec. Order No. 13292, Sec. 4.1(a).

It also is a federal crime to divulge to an unauthorized person specified categories of classified information, including information "concerning the communication intelligence activities of the United States." 18 U.S.C. § 798(a). The term "classified information" means "information which, at the time of a violation of this section, is, for reasons of national security, specifically designated by a United States Government Agency for limited or restricted dissemination or distribution," while an "unauthorized person" is "any person who, or agency which, is not authorized to receive information of the categories set forth in subsection (a) of this section, by the President, or by the head of a department or agency of the United States Government which is expressly designated by the President to engage in communication intelligence activities for the United States." 18 U.S.C. § 798(b).

New Jersey state officials have not been authorized to receive classified information concerning the foreign-intelligence activities of the United States in accordance with the terms of the foregoing statutes or Executive Orders (or any other lawful authority). To the extent your subpoenas seek to compel disclosure of such information to state officials, responding to them would obviously violate federal law.

⁴ Section 6 reflects a "congressional judgment that in order to preserve national security, information elucidating the subjects specified ought to be safe from forced exposure." *The Founding Church of Scientology of Washington, D.C., Inc. v. Nat'l Security Agency*, 610 F.2d 824, 828 (D.C. Cir. 1979); accord *Hayden v. Nat'l Security Agency*, 608 F.2d 1381, 1389 (D.C. Cir. 1979). Thus, in enacting Section 6, Congress was "fully aware of the 'unique and sensitive' activities of the [NSA] which require 'extreme security measures,'" *Hayden*, 608 F.2d at 1390 (citing legislative history), and "[t]he protection afforded by section 6 is, by its very terms, absolute. If a document is covered by section 6, NSA is entitled to withhold it. . . ." *Linder v. Nat'l Security Agency*, 94 F.3d 693, 698 (D.C. Cir. 1996).

The Honorable Zulima V. Farber
Page 5

3. The recent assertion of the state secrets privilege by the Director of National Intelligence ("DNI") in cases regarding the very same topics and types of information sought by your subpoenas underscores that compliance with those subpoenas would be improper. It is well-established that intelligence information relating to the national security of the United States is subject to the Federal Government's state secrets privilege. See *United States v. Reynolds*, 345 U.S. 1 (1953). The privilege encompasses a range of matters, including information the disclosure of which would result in an "impairment of the nation's defense capabilities, disclosure of intelligence-gathering methods or capabilities, and disruption of diplomatic relations with foreign Governments." *Ellsberg v. Mitchell*, 709 F.2d 51, 57 (D.C. Cir. 1983), cert. denied sub nom. *Russo v. Mitchell*, 465 U.S. 1038 (1984) (footnotes omitted); see also *Halkin v. Helms*, 690 F.2d 977, 990 (D.C. Cir. 1982) (state secrets privilege protects intelligence sources and methods involved in NSA surveillance).

In ongoing litigation in the United States District Court for the Northern District of California, the DNI has formally asserted the state secrets privilege regarding the very same topics and types of information sought by your subpoenas. See *Hepting v. AT&T Corp.*, No. 06-0672-VRW (N.D. Cal.). In particular, the DNI's assertion of the privilege encompasses "allegations about NSA's purported involvement with AT&T," Negroponte Decl. ¶12, because "[t]he United States can neither confirm nor deny allegations concerning intelligence activities, sources, methods, relationships, or targets." *Id.* ¶ 12. As DNI Negroponte has explained, "[t]he only recourse for the Intelligence Community and, in this case, for the NSA, is to neither confirm nor deny these sorts of allegations, regardless of whether they are true or false. To say otherwise when challenged in litigation would result in routine exposure of intelligence information, sources, and methods and would severely undermine surveillance activities in general." Negroponte Decl. ¶12; see also Alexander Decl. ¶8. As DNI Negroponte has further explained, to disclose further details about the intelligence activities of the United States "would disclose classified intelligence information and reveal intelligence sources and methods, which would enable adversaries of the United States to avoid detection by the U.S. Intelligence Community and/or take measures to defeat or neutralize U.S. intelligence collection, posing a serious threat of damage to the United States' national security interests." Negroponte Decl. ¶ 11. Those concerns are particularly acute when we are facing the threat of terrorist attacks on United States soil.

In seeking information bearing upon NSA's purported involvement with various telecommunications carriers, your subpoenas thus seek the disclosure of matters with respect to which the DNI already has determined that disclosure, including confirming or denying whether or to what extent such materials exist, would improperly reveal intelligence sources and methods. Accordingly, the state law upon which the subpoenas are based is inconsistent with and preempted by federal law as regards intelligence gathering, and also conflicts with the assertion of the state secrets privilege by the Director of National Intelligence. Any application of state law that would compel such disclosures notwithstanding the DNI's assessment would contravene

The Honorable Zulima V. Farber
Page 6

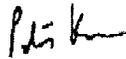
the DNI's authority and the Act of Congress conferring that authority. More broadly, the subpoenas involve an improper effort to use state law to regulate or oversee federal functions, and implicate federal immunity under the Supremacy Clause.

* * *

For the reasons outlined above, the United States believes that the subpoenas and the application of state law they embody are plainly inconsistent with and preempted under the Supremacy Clause, and that compliance with the subpoenas would place the carriers in a position of having to confirm or deny the existence of information that cannot be confirmed or denied without causing harm to the national security. In this light, we sincerely hope that you will withdraw the subpoenas, so that litigation over this matter may be avoided.

Please do not hesitate to contact me if you have any questions. As noted, your consideration of this matter is very much appreciated.

Sincerely,



Peter D. Keisler

cc: Bradford A. Berenson, Esq.
John G. Kester, Esq.
John A. Rogovin, Esq.
Christine A. Varney, Esq.

Attachments

EXHIBIT M



IMPORTANT: This facsimile is intended only for the use of the individual or entity to which it is addressed. It may contain information that is privileged, confidential, or otherwise protected from disclosure under applicable law. If the reader of this transmission is not the intended recipient or the employee or agent responsible for delivering the transmission to the intended recipient, you are hereby notified that any dissemination, distribution, copying or use of this transmission or its contents is strictly prohibited. If you have received this transmission in error, please notify us by telephoning and return the original transmission to us at the address given below.

FROM: Department of Justice
Civil Division
Room 3141
950 Pennsylvania Avenue, N.W.
Washington, D.C. 20530

DATE: June 14, 2006

FAX NO.: 514.8071
DIRECT DIAL: 514.3301

SENT BY: Peter D. Keisler
Assistant Attorney General

TO: Bradley A. Berenson, Esq. 736.8711
John G. Kester, Esq. 434.5060
John A. Rogovin, Esq. 663.6363
Christine A. Varney, Esq. 637.5910

NUMBER OF PAGES SENT (INCLUDING COVER PAGE): 56

(Part I)

SPECIAL INSTRUCTIONS:



U. S. Department of Justice

Civil Division

Assistant Attorney General

Washington, D.C. 20530

June 14, 2006

VIA FACSIMILE AND EMAIL

Bradford A. Berenson, Esq.
Sidley Austin LLP
1501 K Street, NW
Washington, D.C. 20005

John A. Rogovin, Esq.
Wilmer Hale
1875 Pennsylvania Avenue, NW
Washington, D.C. 20006

John G. Kester, Esq.
Williams & Connolly LLP
725 Twelfth Street, NW
Washington, D.C. 20005

Christine A. Varney, Esq.
Hogan & Hartson LLP
555 Thirteenth Street, NW
Washington, D.C. 20004

**Re: Subpoenas Duces Tecum Served on Telecommunications Carriers
Seeking Information Relating to the Alleged Provision of Telephone
Call History Data to the National Security Agency**

Dear Counsel:

This letter is to advise you that today the United States of America has filed a lawsuit against the Attorney General and other officials of the State of New Jersey, as well as AT&T Corp., Verizon Communications, Inc., Qwest Communications International, Inc., Sprint Nextel Corporation, and Cingular Wireless LLC (together the "telecommunications carriers"). That lawsuit seeks a declaration that those state officials do not have the authority to enforce subpoenas duces tecum (hereafter the "subpoenas") recently issued to the telecommunications carriers seeking information relating to the alleged provision of "telephone call history data" to the National Security Agency, and that the telecommunications carriers cannot respond to these subpoenas. A copy of the Complaint the United States has filed, as well as a letter we have sent today to Attorney General Farber, are attached hereto.

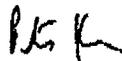
As noted in our Complaint and letter to Attorney General Farber concerning those issues, the subpoenas infringe upon federal operations, are contrary to federal law, and are invalid under the Supremacy Clause of the United States Constitution. Responding to the subpoenas – including by disclosing whether or to what extent any responsive materials exist – would violate federal laws and Executive Orders. Moreover, the Director of National Intelligence recently has asserted the state secrets privilege with respect to the very same topics and types of information sought by the subpoenas, thereby underscoring that any such information cannot be disclosed. For these reasons, described in more detail in the attachments hereto, please be advised that we

Messrs. Berenson, Kester, Rogovin, Ms. Varney
Page 2

believe that enforcing compliance with, or responding to, the subpoenas would be inconsistent with and preempted by federal law.

Please do not hesitate to contact Carl Nichols or me should you have any questions in this regard.

Sincerely,



Peter D. Keisler
Assistant Attorney General

Attachments