PETER D. KEISLER
Assistant Attorney General, Civil Division
CARL J. NICHOLS
Deputy Assistant Attorney General
DOUGLAS N. LETTER
Terrorism Litigation Counsel
JOSEPH H. HUNT
Director, Federal Programs Branch
ANTHONY J. COPPOLINO
Special Litigation Counsel
tony.coppolino@usdoj.gov
ANDREW H. TANNENBAUM
andrew.tannenbaum@usdoj.gov
Trial Attorney
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

Attorneys for Intervenor Defendant United States of America

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 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

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

Respectfully submitted,

PETER D. KEISLER
Assistant Attorney General, Civil Division

CARL J. NICHOLS
Deputy Assistant Attorney General

DOUGLAS N. LETTER
Terrorism Litigation Counsel

JOSEPH H. HUNT
Director, Federal Programs Branch

s/Anthony J. Coppolino
ANTHONY J. COPPOLINO
Special Litigation Counsel
tony.coppolino@usdoj.gov

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

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

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

PETER D. KEISLER
Assistant Attorney General
CARL J. NICHOLS
Deputy Assistant Attorney General
DOUGLAS N. LETTER
Terrorism Litigation Counsel
JOSEPH H. HUNT
Director, Federal Programs Branch
ANTHONY J. COPPOLINO
Special Litigation Counsel
tony.coppolino@usdoj.gov
ANDREW H. TANNENBAUM
andrew.tannenbaum@usdoj.gov
Trial Attorney
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
Attorneys for the United States of America

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 **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

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

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

---

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

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

[3] **(U)** The classified declarations of John D. Negroponte, DNI, and Keith B. Alexander, 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.

[REDACTED TEXT]

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

[REDACTED TEXT]

(U) BACKGROUND

A. (U) September 11, 2001

(U) 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. Those operatives targeted the Nation's financial center in New York with two of the

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

(U) 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. 48199 (Sept. 14, 2001). The United States also launched a massive 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 training grounds and haven in Afghanistan. On September 14, 2001, both Houses of 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 11. Authorization for Use of Military Force, Pub. L. No. 107-40 § 21(a), 115 Stat. 224, 224 (Sept. 18, 2001) ("Cong. Auth."). 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 acknowledged in particular that the "the President has authority under the Constitution to take action to deter and prevent acts of international terrorism against the United States." *Id.* pmbl.

(U) As the President made clear at the time, the attacks of September 11 "created a state of armed conflict." Military Order, § 1(a), 66 Fed. Reg. 57833, 57833 (Nov. 13, 2001). Indeed, shortly after the attacks, NATO took the unprecedented step of invoking 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 that al Qaeda terrorists "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 he concluded that "an extraordinary emergency exists for national defense purposes." Military Order, § 1(c), (g), 66 Fed. Reg. at 57833-34.

B. (U) The Continuing Terrorist Threat Posed by al Qaeda

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

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

(U) Since the September 11 attacks, al Qaeda leaders have repeatedly promised to deliver another, even more devastating attack on America. For example, in October 2002, al Qaeda leader Ayman al-Zawahiri stated in a video addressing the "citizens of the United States": "I promise you that the Islamic youth are preparing for you what will fill your hearts with horror." In October 2003, Osama bin Laden stated in a released videotape that "We, God willing, will continue to fight you and will continue martyrdom operations inside and outside the United States . . . ." And again in a videotape released on October 24, 2004, bin Laden warned U.S. citizens of further attacks and asserted that "your security is in your own hands." In recent months, al Qaeda has reiterated its intent to inflict a catastrophic terrorist attack on the United States. On December 7, 2005, 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." Finally, as is well known, since September 11, al Qaeda has staged several large-scale attacks around the world, including in Indonesia, Madrid, and London, killing hundreds of innocent people.

[REDACTED TEXT]

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

[REDACTED TEXT]

---

[4] **(U)** Available at http://www.white-house.gov//news/releases/2005/12/20051219-2.html.

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

[REDACTED TEXT]

E. (U) Plaintiffs' Claims

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

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

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

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

(U) ARGUMENT

[REDACTED TEXT]

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

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

A. (U) Procedural Requirements

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

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

B. (U) Information Covered

(U) The privilege protects a broad range of state secrets, including information that would result in "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); *accord Kasza*, 133 F.3d at 1166 ("[T]he Government may use the state secrets privilege to withhold a broad range of information;"); *see also Halkin v. Helms* (*Halkin II*), 690 F.2d 977, 990 (D.C. Cir. 1982) (state secrets privilege protects intelligence sources and methods involved in NSA surveillance). In addition, the privilege extends to protect information that, on its face, may appear innocuous but which in a larger context could reveal sensitive classified information. *Kasza*, 133 F.3d at 1166.

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

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

C. (U) Standard of Review

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

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

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

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

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

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

> It is not to slight judges, lawyers or anyone else to suggest that any such 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)).

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

General's formal invocation of state secrets privilege).

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

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

(U) It cannot be disputed that the United States properly has asserted the state secrets privilege in this case. The Director of National Intelligence, who bears statutory authority as head of the United States Intelligence Community to protect intelligence sources and methods, *see* 50 U.S.C. § 403-1(i)(l), has formally asserted the state secrets privilege after personal consideration of the matter. *See Reynolds*, 345 U.S. at 7-8.[5] DNI Negroponte has submitted an unclassified declaration and an *in camera*, *ex parte* classified declaration, both of which state that the disclosure of the intelligence information, sources, and methods described herein would cause exceptionally grave harm to the national security of the United States. *See* Public and *In Camera, Ex Parte* Declarations of John D. Negroponte, Director of National Intelligence. Based on this assertion of privilege by the head of the United States intelligence community, the Government's claim of privilege has been properly lodged.

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

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

---

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

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

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

[REDACTED TEXT]

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

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

(U) Two statutory protections also apply to the intelligence-related information, sources and methods described herein, and both have been properly invoked here as well. First, 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 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.

Id. 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). 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). Thus, "[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).

(U) The second applicable statute is 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). This statute requires the Director of National Intelligence to "protect intelligence sources and methods from unauthorized disclosure. 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." *Snepp 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], not that of the judiciary 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.

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

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

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

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

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

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

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

[REDACTED TEXT]

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

[REDACTED TEXT]

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

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

1. (U) Plaintiffs Cannot Establish Standing

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

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

(U) Plaintiffs cannot prove these elements without information covered by the state secrets assertion.[8] The Government's privilege assertion covers any information tending to

---

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

[7] **(U)** Standing requirements demand the "strictest adherence" when, like here, constitutional questions are presented and "matters of great national significance are at stake." *Elk Grove Unified Sch. Dist. v. Newdow*, 542 U.S. 1, 11 (2004); *see also Raines v. Byrd*, 521 U.S. 811, 819-20 (1997) ("[O]ur standing inquiry has been especially rigorous when reaching the merits of the dispute would force us to decide whether an action taken by one of the other two branches of the Federal Government was unconstitutional."); *Schlesinger v. Reservists Comm. to Stop the War*, 418 U.S. 208, 221 (1974) ("[W]hen a court is asked to undertake constitutional 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.").

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

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

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

---

argument that the acquisition of a plaintiff's communications may be presumed from the 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").

[9] **(U)** To the extent Plaintiffs challenge the TSP, *see, e.g.,* Am. Compl. 32-37, their allegations are insufficient on their face to establish standing even apart from the state secrets issue because Plaintiffs fail to demonstrate that they fall anywhere near the scope of that 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 agents of foreign powers, "including without limitation anyone who knowingly engages in 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 subscriber who falls *outside* the narrow scope of the TSP but nonetheless disagrees with the program. Such a generalized grievance is clearly insufficient to support either constitutional or prudential standing to challenge the TSP. *See Halkin II*, 690 F.2d at 1001-03 (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 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.

Circuit upheld an assertion of the state secrets privilege regarding the identities of individuals subject to NSA surveillance, rejecting the plaintiffs' argument that the privilege could not extend to the "mere fact of interception," *id.* at 8, and despite significant public disclosures about the surveillance activities at issue, *id.* at 10.[10] A similar state secrets assertion with respect to the identities of individuals subject to CIA surveillance was upheld in *Halkin II*. *See* 690 F.2d at 991. As a result of these privilege assertions in both *Halkin I* and *Halkin II*, the D.C. Circuit held that the plaintiffs were incapable of demonstrating that they had standing to challenge the alleged surveillance. *See id.* at 997.[11] Significantly, the court held that the fact of such surveillance could not be proven even if the CIA had actually requested NSA to intercept the plaintiffs' communications by including their names on a "watchlist" sent to NSA—a fact which was not covered by the state secrets assertion in that case. *See id.* at 999-1000 ("[T]he absence of proof of actual acquisition of appellants' communications is fatal to their watchlisting claims."). The court thus found dismissal warranted, even though the complaint alleged actual interception of

---

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

[11] **(U)** *See Halkin II*, 690 F.2d at 998 ("We hold that appellants' inability to adduce proof of actual acquisition of their communications now prevents them from stating a cognizable claim in the federal courts. In particular, we find appellants incapable of making the showing necessary to establish their standing to seek relief."); *id.* at 997 (quoting district court's ruling that "plaintiffs cannot show any injury from having their names submitted to NSA because NSA is prohibited from disclosing whether it acquired any of plaintiffs' communications"); *id.* at 990 ("Without access to the facts about the identities of particular plaintiffs who were subjected to CIA surveillance (or to NSA interception at the instance of the CIA), direct injury in fact to any 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.").

plaintiffs' communications, because the plaintiffs' alleged injuries could be no more than speculative in the absence of their ability to prove that such interception occurred. *Id.* at 999, 1001.[12]

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

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

---

[12] **(U)** Because the CIA conceded that nine plaintiffs were subjected to certain types of non-NSA surveillance, the D.C. Circuit held that those plaintiffs had demonstrated an injury-in-fact. *See Halkin II*, 690 F.2d at 1003. Nonetheless, the nine plaintiffs were precluded from 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.

[13] **(U)** Plaintiffs cannot overcome this fundamental standing bar simply by alleging that their speech has been chilled as the result of their own subjective fear of Government surveillance. *See* Plaintiffs' Memorandum of Points and Authorities in Support of Motion for Preliminary Injunction at 25. Specifics about this alleged chilling effect are provided with 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

[REDACTED TEXT]

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

[REDACTED TEXT]

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

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

"self-censorship" makes any sense in light of the acknowledged limitation of the TSP to international communications actually conducted by al Qaeda-affiliated individuals, as opposed to a mass targeting of particular *topics* of conversation or research. *Id.* In any event, Plaintiffs' claim of a chilling effect is foreclosed by *Laird v. Tatum*, 408 U.S. 1 (1972), which squarely 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).

> Notwithstanding any other law, providers of wire or electronic communication service, their officers, employees, and agents, landlords, custodians, or other persons, are authorized to provide information, facilities, or technical assistance to persons authorized by law to intercept wire, oral, or electronic communications or to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, if such provider, its officers, employees, or agents, landlord, custodian, or other specified person, has been provided with—
> (A) a court order directing such assistance signed by the authorizing judge, or
> (B) a certification in writing by a person specified in 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.

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

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

18 U.S.C. § 2511(2)(a)(ii).[14]

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

---

[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").

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

[REDACTED TEXT]

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

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

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

[REDACTED TEXT]

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

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

(U) For example, both before and after the enactment of the Foreign Intelligence Surveillance Act, every federal appellate court to consider the issue 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).

(U) In *United States v. United States District Court,* 407 U.S. 297 (1972) ("*Keith*"), 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 made clear that it was not addressing the President's authority to

conduct *foreign* intelligence surveillance (even within the United States) 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.").[15] 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 has 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. As one court put it:

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

---

[15] **(U)** *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.

Butenko, 494 F.2d 605.

(U) Beyond this, the Supreme Court has held that the warrant requirement is inapplicable in situations involving "special needs" that go beyond a routine interest in law enforcement. *Vernonia Sch. Dist. v. Acton,* 515 U.S. 646, 653 (1995) (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)); *Illinois v. McArthur*, 531 U.S. 326, 330 (2001) ("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."). 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 interests in public safety beyond the interests in ordinary law enforcement are at stake. *See, e.g., Skinner v. Railway Labor Executives' Ass'n*, 489 U.S. 602, 634 (1989) (drug testing of railroad personnel involved in train accidents). As should be apparent, demonstrating that this body of law applies to a particular case requires reference to specific facts.

[REDACTED TEXT]

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

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

[REDACTED TEXT]

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

[REDACTED TEXT]

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

---

[16] **(U)** *See also Halkin II*, 690 F.2d at 1000 ("Determining the reasonableness of 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.").

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

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

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

[REDACTED TEXT]

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

statutory and constitutional authority to gather intelligence information about foreign enemies. *See, e.g., Totten v. United States*, 92 U.S. 105, 106 (1876) (recognizing President's authority to hire spies); *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."). And, as noted, courts have held that the President has inherent constitutional authority to authorize foreign intelligence surveillance. *See supra.*

[REDACTED TEXT]

(U) CONCLUSION

For the foregoing reasons, the Court should:

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

2. Dismiss this action 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.

Respectfully submitted,

PETER D. KEISLER
Assistant Attorney General

CARL J. NICHOLS
Deputy Assistant Attorney General

DOUGLAS N. LETTER
Terrorism Litigation Counsel

JOSEPH H. HUNT
Director, Federal Programs Branch

s/ Anthony J. Coppolino
ANTHONY J. COPPOLINO
Special Litigation Counsel
tony.coppolino@usdoj.gov

s/ Andrew H. Tannenbaum
ANDREW H. TANNENBAUM
Trial Attorney
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

Attorneys for United States of America

DATED: May 12, 2006

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