

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

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.

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

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 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
 7 tony.coppolino@usdoj.gov
 ANDREW H. TANNENBAUM
 8 andrew.tannenbaum@usdoj.gov
 9 Trial Attorney
 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

14 UNITED STATES DISTRICT COURT

15 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

15 (U) In addition, the United States has also moved to intervene in this action, pursuant to
16 Rule 24 of the Federal Rules of Civil Procedure, for the purpose of seeking dismissal of this
17 action or, in the alternative, summary judgment. As set forth below, this case cannot be litigated
18 because adjudication of Plaintiffs’ claims would put at risk the disclosure of privileged national
19 security information.
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 (U) As the President made clear at the time, the attacks of September 11 “created a state
6 of armed conflict.” Military Order, § 1(a), 66 Fed. Reg. 57833, 57833 (Nov. 13, 2001). Indeed,
7 shortly after the attacks, NATO took the unprecedented step of invoking article 5 of the North
8 Atlantic Treaty, which provides that an “armed attack against one or more of [the parties] shall
9 be considered an attack against them all.” North Atlantic Treaty, Apr. 4, 1949, art. 5, 63 Stat.
10 2241, 2244, 34 U.N.T.S. 243, 246; see also Statement by NATO Secretary General Lord
11 Robertson (Oct. 2, 2001), available at <http://www.nato.int/docu/speech/2001/s011002a.htm> (“[I]t
12 has now been determined that the attack against the United States on 11 September was directed
13 from abroad and shall therefore be regarded as an action covered by Article 5 of the Washington
14 Treaty . . .”). The President also determined that al Qaeda terrorists “possess both the capability
15 and the intention to undertake further terrorist attacks against the United States that, if not
16 detected and prevented, will cause mass deaths, mass injuries, and massive destruction of
17 property, and may place at risk the continuity of the operations of the United States
18 Government,” and he concluded that “an extraordinary emergency exists for national defense
19 purposes.” Military Order, § 1(c), (g), 66 Fed. Reg. at 57833-34.
20
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

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

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.

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

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

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
28

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)(1), 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").

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.

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.

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:

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,
salaries, or number of persons employed by such agency.

23 *Id.* Section 6 reflects a “congressional judgment that in order to preserve national security,
24 information elucidating the subjects specified ought to be safe from forced exposure.” *The*
25 *Founding Church of Scientology of Washington, D.C., Inc. v. Nat’l Security Agency*, 610 F.2d
26 824, 828 (D.C. Cir. 1979); *accord Hayden v. Nat’l Security Agency*, 608 F.2d 1381, 1389 (D.C.
27 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 [REDACTED TEXT]

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

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
 17 individual defendants who would have no way to rebut it").

18 ⁹ (U) To the extent Plaintiffs challenge the TSP, *see, e.g.*, Am. Compl. 32-37, their
 19 allegations are insufficient on their face to establish standing even apart from the state secrets
 20 issue because Plaintiffs fail to demonstrate that they fall anywhere near the scope of that
 21 program. Plaintiffs do not claim to be, or to communicate with, members or affiliates of al
 22 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.
 25 ¶ 70. The named Plaintiffs thus are in no different position from any other citizen or AT&T
 26 subscriber who falls *outside* the narrow scope of the TSP but nonetheless disagrees with the
 27 program. Such a generalized grievance is clearly insufficient to support either constitutional or
 28 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.

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.

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

16
 17
 18
 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
 24 future injury or a live controversy in light of the fact that the CIA had terminated the specific
 25 intelligence methods at issue. *See id.* at 1005–09.

26 ¹³ (U) Plaintiffs cannot overcome this fundamental standing bar simply by alleging that
 27 their speech has been chilled as the result of their own subjective fear of Government
 28 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

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).

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 [REDACTED TEXT]

7
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 [REDACTED TEXT]

27
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.

21 ¹⁵ (U) *Keith* made clear that one of the significant concerns driving the Court’s
 22 conclusion in the domestic security context was the inevitable connection between perceived
 23 threats to domestic security and political dissent. As the Court explained: “Fourth Amendment
 24 protections become the more necessary when the targets of official surveillance may be those
 25 suspected of unorthodoxy in their political beliefs. The danger to political dissent is acute where
 26 the Government attempts to act under so vague a concept as the power to protect ‘domestic
 27 security.’” *Keith*, 407 U.S. at 314; *see also id.* at 320 (“Security surveillances are especially
 28 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
 17 **[REDACTED TEXT]**

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

21 **[REDACTED TEXT]**

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

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.

1 Respectfully submitted,

2 PETER D. KEISLER
Assistant Attorney General

3
4 CARL J. NICHOLS
Deputy Assistant Attorney General

5
6 DOUGLAS N. LETTER
Terrorism Litigation Counsel

7
8 JOSEPH H. HUNT
Director, Federal Programs Branch

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

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

19 Attorneys for United States of America

20 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