

EXHIBIT 6

MDL 1791

JUDICIAL PANEL ON
MULTIDISTRICT LITIGATION

AUG - 9 2006

RELEASED FOR PUBLICATION

FILED
CLERK'S OFFICE

DOCKET NO. 1791

BEFORE THE JUDICIAL PANEL ON MULTIDISTRICT LITIGATION

**IN RE NATIONAL SECURITY AGENCY TELECOMMUNICATIONS
RECORDS LITIGATION**

**BEFORE WM. TERRELL HODGES, CHAIRMAN, D. LOWELL JENSEN, J.
FREDERICK MOTZ,* ROBERT L. MILLER, JR.,* KATHRYN H. VRATIL,
DAVID R. HANSEN AND ANTHONY J. SCIRICA, JUDGES OF THE PANEL**

TRANSFER ORDER

This litigation currently consists of seventeen actions listed on the attached Schedule A and pending in thirteen districts as follows: three actions in the District of Rhode Island; two actions each in the Northern District of Illinois and the District of Montana; and one action each in the Eastern, Northern and Southern Districts of California, the Eastern District of Louisiana, the Eastern and Southern Districts of New York, the District of Oregon, the Middle District of Tennessee, and the Southern and Western Districts of Texas.¹ Defendant Verizon Communications Inc. and two of its affiliates move the Panel, pursuant to 28 U.S.C. § 1407, for an order centralizing the MDL-1791 actions in the District of District of Columbia. In the filed responses to the motion, plaintiffs in four actions opposed inclusion of their actions in any Section 1407 centralization, and plaintiffs in a potential tag-along action favored separate centralization of what they identified as two distinct subsets of actions encompassed in the motion before the Panel and in the list of various actions that have been identified as potential tag-along actions. All other respondents supported transfer, differing among themselves only with respect to selection of the transferee district. Defendants AT&T Corp., BellSouth Corp. (and two of its affiliates), and the United States joined the movants in supporting selection of the District of District of Columbia as transferee district. The responding plaintiffs who supported transfer offered

*Judges Motz and Miller took no part in the decision of this matter.

¹The Section 1407 motion, as originally filed, also pertained to three additional actions that were then pending in the District of District of Columbia. Subsequently the plaintiffs in those three actions voluntarily dismissed their complaints, thus mooted the question of Section 1407 transfer with respect to those actions. Additionally, parties have notified the Panel of 26 potentially related actions recently filed in eighteen districts as follows: four actions each in the Northern District of California and the Southern District of New York; two actions each in the Northern District of Georgia and the Southern District of Indiana; and one action each in the Southern District of Florida, the District of Hawaii, the Northern District of Illinois, the Western District of Kentucky, the Eastern District of Louisiana, the Eastern and Western Districts of Michigan, the Eastern District of Missouri, the District of New Jersey, the Eastern District of New York, the District of Oregon, the Eastern District of Pennsylvania, the Western District of Texas, and the Western District of Washington. In light of the Panel's disposition of this docket, these actions will be treated as potential tag-along actions in accordance with Panel and local court rules. See Rules 7.4 and 7.5, R.P.J.P.M.L., 199 F.R.D. 425, 435-36 (2001).

OFFICIAL FILE COPY

IMAGED AUG - 9 2006

PLEADING NO. 51

an array of other forum choices: the Northern District of California, the Northern District of Illinois, the Eastern District of Louisiana, the Southern District of New York, and the District of Rhode Island. By the time of the Panel's hearing session, most responding plaintiffs were in agreement that the Northern District of California should be selected as the transferee forum if the Panel ordered centralization in this docket.

On the basis of the papers filed and hearing session held, the Panel finds that these actions involve common questions of fact, and that centralization under Section 1407 in the Northern District of California will serve the convenience of the parties and witnesses and promote the just and efficient conduct of this litigation. All actions are purported class actions sharing factual and legal questions regarding alleged Government surveillance of telecommunications activity and the participation in (or cooperation with) that surveillance by individual telecommunications companies. Centralization under Section 1407 is necessary in order to eliminate duplicative discovery, prevent inconsistent pretrial rulings (particularly with respect to matters involving national security), and conserve the resources of the parties, their counsel and the judiciary.

Some parties oppose transfer because they view their actions to be more narrowly drawn (such as with respect to breadth of defendants, nature of alleged improper conduct, range of legal theories, or type of relief sought) than other MDL-1791 actions, and they thus seek to avoid entanglement in a litigation which they deem to be broader in scope. Transfer under Section 1407, however, does not require a complete identity or even majority of common factual issues as a prerequisite to transfer. Here, Section 1407 transfer will have the salutary effect of placing all actions in this docket before a single judge who can formulate a pretrial program that: 1) allows discovery with respect to any non-common issues to proceed concurrently with discovery on common issues, *In re Joseph F. Smith Patent Litigation*, 407 F.Supp. 1403, 1404 (J.P.M.L. 1976); and 2) ensures that pretrial proceedings will be conducted in a manner leading to a just and expeditious resolution of the actions to the benefit of not just some but all of the litigation's parties. As Section 1407 proceedings evolve in the transferee district, these parties may at some point wish to renew their arguments that the uniqueness or simplicity of their actions renders continued inclusion of those actions in MDL-1791 unnecessary or inadvisable. They then will be free to approach the transferee judge for a suggestion of remand, and whenever the transferee judge deems remand of any claims or actions appropriate, procedures are available whereby this may be accomplished with a minimum of delay. See Rule 7.6, R.P.J.P.M.L., 199 F.R.D. at 436-38.

We conclude that the Northern District of California is an appropriate transferee forum in this docket because the district is where the first filed and significantly more advanced action is pending before a judge already well versed in the issues presented by the litigation. One of the Government's key arguments for centralization in this docket is its contention that, because of security concerns associated with the production of highly classified information, a framework should be created whereby a single transferee court (rather than the multiple courts where MDL-1791 actions and potential tag-along actions are now pending) would be charged with the task of reviewing any classified information that might need to be produced in connection with the plaintiffs' claims and the Government's assertion

of the state secret defense. In that regard, the California district is one of the two districts in this litigation where a court has already established and utilized a procedure for reviewing classified information that the Government deems necessary to decide its state secret claim. On the other hand, the District of District of Columbia, which is the forum choice of the movants, the Government and other responding defendants, is a district where no constituent MDL-1791 action is now pending. Centralization in the District of Columbia forum would thus require the very duplication and expansion of access to classified information that the Government deems to be so perilous.

IT IS THEREFORE ORDERED that, pursuant to 28 U.S.C. § 1407, the actions listed on Schedule A and pending outside the Northern District of California are transferred to the Northern District of California and, with the consent of that court, assigned to the Honorable Vaughn R. Walker for coordinated or consolidated pretrial proceedings with the action on Schedule A and pending in that district.

FOR THE PANEL:



Wm. Terrell Hodges
Chairman

SCHEDULE A

MDL-1791 -- In re National Security Agency Telecommunications Records Litigation

Eastern District of California

Greg Conner, et al. v. AT&T Corp., et al., C.A. No. 1:06-632

Northern District of California

Tash Hepting, et al. v. AT&T Corp., et al., C.A. No. 3:06-672

Southern District of California

Shelly D. Souder v. AT&T Corp., et al., C.A. No. 3:06-1058

Northern District of Illinois

Steven Schwarz, et al. v. AT&T Corp., et al., C.A. No. 1:06-2680

Studs Terkel, et al. v. AT&T Inc., C.A. No. 1:06-2837

Eastern District of Louisiana

Tina Herron, et al. v. Verizon Global Networks, Inc., et al., C.A. No. 2:06-2491

District of Montana

Rhea Fuller v. Verizon Communications, Inc., et al., C.A. No. 9:06-77

Steve Dolberg v. AT&T Corp., et al., C.A. No. 9:06-78

Eastern District of New York

Edward Marck, et al. v. Verizon Communications, Inc., C.A. No. 2:06-2455

Southern District of New York

Carl J. Mayer, et al. v. Verizon Communications Inc., et al., C.A. No. 1:06-3650

District of Oregon

Darryl Hines v. Verizon Northwest, Inc., C.A. No. 3:06-694

MDL-1791 Schedule A (Continued)

District of Rhode Island

Charles F. Bissit, et al. v. Verizon Communications, Inc., et al., C.A. No. 1:06-220

Pamela A. Mahoney v. AT&T Communications, Inc., C.A. No. 1:06-223

Pamela A. Mahoney v. Verizon Communications, Inc., C.A. No. 1:06-224

Middle District of Tennessee

Kathryn Potter v. BellSouth Corp., C.A. No. 3:06-469

Southern District of Texas

Mary J. Trevino, et al. v. AT&T Corp., et al., C.A. No. 2:06-209

Western District of Texas

James C. Harrington, et al. v. AT&T Inc., C.A. No. 1:06-374

EXHIBIT 7

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

7 SIDLEY AUSTIN LLP
 DAVID W. CARPENTER (admitted *pro hac vice*)
 8 DAVID L. LAWSON (admitted *pro hac vice*)
 BRADFORD A. BERENSON (admitted *pro hac vice*)
 9 EDWARD R. McNICHOLAS (admitted *pro hac vice*)
 1501 K Street, N.W.
 10 Washington, D.C. 20005
 Telephone: (202) 736-8010
 11 Facsimile: (202) 736-8711
 Email: bberenson@sidley.com
 12
 Attorneys for Defendants
 13 AT&T CORP. and AT&T INC.

14 UNITED STATES DISTRICT COURT
 15 NORTHERN DISTRICT OF CALIFORNIA
 16 SAN FRANCISCO DIVISION

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

20 Plaintiffs,

21 vs.

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

24 Defendants.

No. C-06-0672-VRW

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

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

Filed concurrently:

1. Request for judicial notice
2. Proposed order

1 **TABLE OF CONTENTS**

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

3 ISSUES TO BE DECIDED..... vi

4 MEMORANDUM OF POINTS AND AUTHORITIES..... 1

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

6 II. SUMMARY OF THE CASE..... 2

7 A. Background..... 2

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

9 III. ARGUMENT..... 4

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

11 FROM SUIT..... 4

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

13 immunity..... 5

14 a. Numerous statutes provide telecommunications

15 carriers absolute immunity for assisting governmental

16 activities..... 5

17 b. Plaintiffs have the burden of pleading facts sufficient

18 to avoid these immunities..... 7

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

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

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

22 immunity..... 13

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

24 of law..... 15

25 B. PLAINTIFFS LACK STANDING..... 19

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

27 2. Plaintiffs' dissatisfaction with government policy does not

28 give them standing..... 22

3. Plaintiffs fail to allege concrete injuries to their statutory

interests..... 24

IV. CONCLUSION..... 255

TABLE OF AUTHORITIES

CASES

1

2

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

4

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

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

7

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

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

10

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

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

13

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

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

16

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

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

19

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

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

22

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

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

25

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

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

28

1	<i>Halkin v. Helms</i> , 690 F.2d 977 (D.C. Cir. 1982).....	21
2		
3	<i>Halperin v. Kissinger</i> , 424 F. Supp. 838 (D.D.C. 1976), <i>rev'd on other grounds</i> , 606 F.2d 1192 (D.C. Cir.1979).....	14, 15
4		
5	<i>Harlow v. Fitzgerald</i> , 457 U.S. 800 (1982).....	16
6	<i>Hodgers-Durgin v. de la Vina</i> , 199 F.3d 1037 (9th Cir. 1999).....	19
7		
8	<i>Hunter v. Bryant</i> , 502 U.S. 224 (1991).....	16
9	<i>In re Sealed Case</i> , 310 F.3d 717 (FISA Ct. Rev. 2002).....	12, 18
10		
11	<i>In re VeriFone Sec. Litigation</i> , 11 F.3d 865 (9th Cir. 1993).....	4
12	<i>In re World War II Era Japanese Forced Labor Litigation</i> , 164 F. Supp. 2d 1160 (N.D. Cal. 2001).....	23, 24
13		
14	<i>Jacobson v. Rose</i> , 592 F.2d 515 (9th Cir. 1978).....	12, 20
15	<i>Kokonnen v. Guardian Life Insurance Co. of America</i> , 511 U.S. 375 (1994).....	4
16		
17	<i>Laird v. Tatum</i> , 408 U.S. 1 (1972).....	22, 23
18	<i>Lujan v. Defenders of Wildlife</i> , 504 U.S. 555 (1992).....	19, 21, 23
19		
20	<i>Mejia v. City of New York</i> , 119 F. Supp. 2d 232 (E.D.N.Y. 2000).....	17
21	<i>O'Shea v. Littleton</i> , 414 U.S. 488 (1974).....	19, 23, 24
22		
23	<i>Raines v. Byrd</i> , 521 U.S. 811 (1997).....	19
24	<i>Richardson v. McKnight</i> , 521 U.S. 399 (1997).....	16, 17
25		
26	<i>Rush v. FDIC</i> , 747 F. Supp. 575 (N.D. Cal. 1990).....	16
27	<i>Schlesinger v. Reservists Committee to Stop the War</i> , 418 U.S. 208 (1974).....	23
28		

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

2

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

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

5

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

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

8

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

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

11

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

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

14

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

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

17

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

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

20

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

22

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

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

25

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

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

28

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

2

3

4

STATUTES AND OTHER AUTHORITY

5 18 U.S.C. § 798(a)(3)..... 10

6 18 U.S.C. § 2511..... passim

7 18 U.S.C. § 2520..... 7, 8, 12

8 18 U.S.C. § 2702..... 6, 9

9 18 U.S.C. § 2703..... 5, 6, 9, 10, 12

10 18 U.S.C. § 3124(d)..... 6

11 47 U.S.C. § 605..... 6, 8, 9

12 50 U.S.C. § 1801..... 24

13 50 U.S.C. § 1805(i)..... 6

14 50 U.S.C. § 1809..... 24

15 50 U.S.C. § 1810..... 24

16 Cal. Bus. & Prof. Code §17200..... 25

17 Cal. Bus. & Prof. Code §17204..... 25

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

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

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

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

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

23

24

25

26

27

28

1 **NOTICE OF MOTION AND MOTION TO DISMISS**

2 **TO ALL PARTIES AND THEIR COUNSEL OF RECORD:**

3 PLEASE TAKE NOTICE that on Thursday, June 8, 2006, at 2:00 p.m., before the
4 Honorable Vaughn R. Walker, United States District Chief Judge, in Courtroom 6,
5 17th Floor, 450 Golden Gate Avenue, San Francisco, California, defendant **AT&T CORP.**
6 ("AT&T") will move and hereby does move, pursuant to Rules 12(b)(1) and 12(b)(6) of the
7 Federal Rules of Civil Procedure, to dismiss the Amended Complaint for Damages,
8 Declaratory and Injunctive Relief (Dkt. 8, referred to hereafter as the "Amended
9 Complaint" or the "FAC") filed by plaintiffs Tash Hepting, Gregory Hicks, Carolyn Jewel
10 and Erik Knutzen (collectively, "plaintiffs") on February 22, 2006.

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

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

18 **ISSUES TO BE DECIDED**

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

23 2. Do the named plaintiffs have standing to challenge alleged government
24 surveillance activities if their complaint does not allege facts—as opposed to unsupported
25 belief—suggesting that they have been or will be the targets of such surveillance?
26
27
28

1 **MEMORANDUM OF POINTS AND AUTHORITIES**

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

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

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

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

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

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

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

20 **A. Background.**

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

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

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

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

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

24

25

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

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

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

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

21 **III. ARGUMENT.**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

25

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

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

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

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

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

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

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

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

(continued...)

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

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

21 (... continued)

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

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

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

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

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

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

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

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

23
24 ⁷ The conclusory allegation that AT&T’s actions were “without lawful authorization,” FAC
25 ¶ 81, cannot meet this burden. In this setting, “a ‘firm application of the Federal Rules of
26 Civil Procedure’ is fully warranted,” including but not limited to “insist[ing] that the
27 plaintiff ‘put forward specific nonconclusory factual allegations’ . . . in order to survive a
28 pre-discovery motion for dismissal or summary judgment.” *Crawford-El*, 523 U.S. at 598
(quoting *Siegert v. Gilley*, 500 U.S. 226, 236 (1991) (Kennedy, J., concurring)). In any
event, FAC ¶ 81 states a legal conclusion that need not be accepted as true on a motion to
dismiss. *Warren*, 328 F.3d at 1139, 1141 n.5.

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

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

21

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

20

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

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

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

17

18

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

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

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

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

28

1 **B. PLAINTIFFS LACK STANDING.**

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

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

27
28

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

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

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

25

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

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

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

23 (... continued)

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

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

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

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

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

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

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

15 Stripped to its essentials, what respondents appear to be seeking is a broad-
16 scale investigation, conducted by themselves as private parties armed with
17 the subpoena power of a federal district court and the power of cross-
18 examination, to probe into the Army's intelligence-gathering activities . . .
19 Carried to its logical end, this approach would have the federal courts as
virtually continuing monitors of the wisdom and soundness of Executive
action.
Laird, 408 U.S. at 14-15.

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

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

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

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

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

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

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

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

9 **IV. CONCLUSION.**

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

11 Dated: April 28, 2006.

12 //

13 //

14 //

15

16

17

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

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

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

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

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

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

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

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

EXHIBIT 8

1 PETER D. KEISLER
 Assistant Attorney General, Civil Division
 2 CARL J. NICHOLS
 Deputy Assistant Attorney General
 3 DOUGLAS N. LETTER
 Terrorism Litigation Counsel
 4 JOSEPH H. HUNT
 Director, Federal Programs Branch
 5 ANTHONY J. COPPOLINO
 Special Litigation Counsel
 6 tony.coppolino@usdoj.gov
 ANDREW H. TANNENBAUM
 7 andrew.tannenbaum@usdoj.gov
 Trial Attorney
 8 U.S. Department of Justice
 Civil Division, Federal Programs Branch
 9 20 Massachusetts Avenue, NW
 Washington, D.C. 20001
 10 Phone: (202) 514-4782/(202) 514-4263
 Fax: (202) 616-8460/(202) 616-8202/(202) 318-2461
 11
 Attorneys for Intervenor Defendant United States of America
 12

13 UNITED STATES DISTRICT COURT
 14 NORTHERN DISTRICT OF CALIFORNIA

15
 16 TASH HEPTING, GREGORY HICKS)
 CAROLYN JEWEL, and ERIK KNUTZEN)
 17 on Behalf of Themselves and All Others)
 Similarly Situated,)
 18
 Plaintiffs,)
 19
 v.)
 20
 21 AT&T CORP., AT&T INC., and)
 22 DOES 1-20, inclusive,)
 23
 Defendants.)
 24

Case No. C 06-0672-VRW

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

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

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

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

9 Respectfully submitted,

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

12 CARL J. NICHOLS
13 Deputy Assistant Attorney General

14 DOUGLAS N. LETTER
15 Terrorism Litigation Counsel

16 JOSEPH H. HUNT
17 Director, Federal Programs Branch

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

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

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.

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

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

Attorneys for Intervenor Defendant United States

DATED: May 12, 2006

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

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

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

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

Case No. C-06-0672-VRW

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

Hon. Vaughn R. Walker

(U) INTRODUCTION

1
2 (U) The United States of America, through its undersigned counsel, hereby submits this
3 Memorandum of Points and Authorities in support of the assertion of the military and state
4 secrets privilege (commonly known as the "state secrets privilege")¹ by the Director of National
5 Intelligence ("DNI"), and related statutory privilege assertions by the DNI and the Director of
6 the National Security Agency ("DIRNSA").² Through these assertions of privilege, the United
7 States seeks to protect certain intelligence activities, information, sources, and methods,
8 implicated by the allegations in this case. The information to be protected is described herein, in
9 a separate memorandum lodged for the Court's *in camera*, *ex parte* consideration, and in public
10 and classified declarations submitted by the DNI and DIRNSA.³ For the reasons set forth in
11 those submissions, the disclosure of the information to which these privilege assertions apply
12 would cause exceptionally grave harm to the national security of the United States.
13
14

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

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

³ (U) The classified declarations of John D. Negrofonte, 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.

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.* p.mbl.

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

22 (U) With the attacks of September 11, Al Qaeda demonstrated its ability to introduce
23 agents into the United States undetected and to perpetrate devastating attacks. But, as the
24 President has made clear, “[t]he terrorists want to strike America again, and they hope to inflict
25
26
27
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 [REDACTED TEXT]
19
20

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

23 [REDACTED TEXT]
24
25
26

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

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.

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

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

10 **(U) ARGUMENT**

11 [REDACTED TEXT]

12
13 **I. (U) THE STATE SECRETS PRIVILEGE BARS USE OF PRIVILEGED INFORMATION REGARDLESS OF A LITIGANT’S NEED.**

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

20
21
22 **A. (U) Procedural Requirements**

23 (U) As a procedural matter, “[t]he privilege belongs to the Government and must be
24 asserted by it; it can neither be claimed nor waived by a private party.” *Reynolds*, 345 U.S. at 7;
25 *see also Kasza*, 133 F.3d at 1165. “There must be a formal claim of privilege, lodged by the
26 head of the department which has control over the matter, after actual personal consideration by
27 the officer.” *Reynolds*, 345 U.S. at 7-8 (footnotes omitted). Thus, the responsible agency head
28

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

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

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

3 (U) The privilege protects a broad range of state secrets, including information that would
4 result in "impairment of the nation's defense capabilities, disclosure of intelligence-gathering
5 methods or capabilities, and disruption of diplomatic relations with foreign Governments."
6 *Ellsberg v. Mitchell*, 709 F.2d 51, 57 (D.C. Cir. 1983), *cert. denied sub nom. Russo v. Mitchell*,
7 465 U.S. 1038 (1984) (footnotes omitted); *accord Kasza*, 133 F.3d at 1166 ("[T]he Government
8 may use the state secrets privilege to withhold a broad range of information;"); *see also Halkin v.*
9 *Helms (Halkin II)*, 690 F.2d 977, 990 (D.C. Cir. 1982) (state secrets privilege protects
10 intelligence sources and methods involved in NSA surveillance). In addition, the privilege
11 extends to protect information that, on its face, may appear innocuous but which in a larger
12 context could reveal sensitive classified information. *Kasza*, 133 F.3d at 1166.

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

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

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

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

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

18
19 **B. (U) The United States Has Demonstrated that There is a Reasonable Danger**
20 **that Disclosure of the Intelligence Information, Sources, and Methods**
21 **Implicated by Plaintiffs' Claims Would Harm the National Security of the**
22 **United States.**

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

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

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

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

8 [REDACTED TEXT]

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

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

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

20 [N]othing in this Act or any other law . . . shall be construed to require the
21 disclosure of the organization or any function of the National Security Agency,
22 of any information with respect to the activities thereof, or of the names, titles,
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'
28

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

1 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
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’
MEMORANDUM OF THE UNITED STATES IN SUPPORT
OF STATE SECRETS PRIVILEGE AND MOTION TO DISMISS
OR, IN THE ALTERNATIVE, FOR SUMMARY JUDGMENT
CASE NO. C-06-0672-VRW

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

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

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

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

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

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

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

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

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

1 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
13
14 (U) The same result is required here. In light of the state secrets assertion, Plaintiffs
15 cannot prove that their communications were intercepted or disclosed by AT&T, and thus they
16 cannot meet their burden to establish standing. Accordingly, like other similar cases before it,
17 this action must be dismissed.¹³
18
19

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

27 ¹³ (U) Plaintiffs cannot overcome this fundamental standing bar simply by alleging that
28 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

1 [REDACTED TEXT]

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

4 [REDACTED TEXT]

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

17
18 (U) In addition to proving actual interception or disclosure to the NSA of their
19 communications, Plaintiffs must also prove, for each of their statutory claims, that any alleged
20 interception or disclosure was not authorized by the Government. In particular, 18 U.S.C.
21 § 2511(2)(a)(ii) provides:
22

23
24 “self-censorship” makes any sense in light of the acknowledged limitation of the TSP to
25 international communications actually conducted by al Qaeda-affiliated individuals, as opposed
26 to a mass targeting of particular *topics* of conversation or research. *Id.* In any event, Plaintiffs'
27 claim of a chilling effect is foreclosed by *Laird v. Tatum*, 408 U.S. 1 (1972), which squarely
28 rejected the assertion of a subjective chill caused by the mere existence of an intelligence
program as a basis to challenge that program. *See* 408 U.S. at 13-14 (“Allegations of a
subjective chill are not an adequate substitute for a claim of specific present objective harm or a
threat of specific future harm.”) (internal quotation marks omitted).

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

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

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

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

19 18 U.S.C. § 2511(2)(a)(ii).¹⁴

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

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

1 activity, acted without Government authorization. This action may be dismissed on that basis
2 alone. See AT&T's Motion to Dismiss Amended Complaint at 7-8. But even if Plaintiffs
3 speculated and alleged the absence of section 2511(2)(a)(ii) authorization, they could not meet
4 their burden of proof on the issue because information confirming or denying AT&T's
5 involvement in alleged intelligence activities is covered by the state secrets assertion.
6

7 [REDACTED TEXT]

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

10 (U) Plaintiffs' Fourth Amendment claim also cannot be proven or defended without
11 information covered by the state secrets assertion. Specifically, Plaintiffs allege that they have a
12 reasonable expectation of privacy in the contents of, and records pertaining to, their
13 communications, and that their rights were violated when AT&T allegedly intercepted or
14 disclosed such communications and records at the instigation of the Government and without
15 lawful authorization. See Am. Compl. ¶¶ 78-89.
16

17 (U) In their preliminary injunction motion, which is focused on Internet communications,
18 Plaintiffs further claim that, "[a]s an agent of the Government," AT&T is engaged in "wholesale
19 copying of vast amounts of communications carried by its WorldNet Internet service." Pls.
20 Prelim. Inj. Mem. at 25. Plaintiffs assert that the alleged surveillance violates the Fourth
21 Amendment because it involves "an automated 'rummaging' through the millions of private
22 communications passing over AT&T's fiber optic network at the discretion of NSA staff." See
23 *id.* at 27. Plaintiffs simply assume that a warrant is required for any and all of the surveillance
24 activities alleged in their Complaint. See *id.*
25
26

27 [REDACTED TEXT]

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

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

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

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

1 conduct *foreign* intelligence surveillance (even within the United States) without a warrant and
2 that it was expressly reserving that question: “[T]he instant case requires no judgment on the
3 scope of the President’s surveillance power with respect to the activities of foreign powers,
4 within or without this country.” *Id.* at 308; *see also id.* at 321-22 & n.20 (“We have not
5 addressed, and express no opinion as to, the issues which may be involved with respect to
6 activities of foreign powers or their agents.”).¹⁵ That *Keith* does not apply in the context of
7 protecting against a foreign attack has been confirmed by the lower courts. After *Keith*, each of
8 the three courts of appeals that have squarely considered the question has concluded—expressly
9 taking the Supreme Court’s decision into account—that the President has inherent authority to
10 conduct warrantless surveillance in the foreign intelligence context. *See, e.g., Truong Dinh*
11 *Hung*, 629 F.2d at 913-14; *Butenko*, 494 F.2d at 603; *Brown*, 484 F.2d 425-26. As one court put
12 it:
13
14

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

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.

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

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

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

21 [REDACTED TEXT]

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

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

5 [REDACTED TEXT]
6

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

16 [REDACTED TEXT]
17

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

25
26
27 ¹⁶ (U) See also *Halkin II*, 690 F.2d at 1000 (“Determining the reasonableness of
28 warrantless foreign intelligence watchlisting under conditions of such informational poverty [due
to the state secrets assertion] . . . would be tantamount to the issuance of an advisory opinion on
the question.”).

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

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

6 (U) Finally, in addition to all of the foregoing issues that could not be litigated
7 without the disclosure of state secrets, adjudication of whether the alleged surveillance activities
8 have been conducted within lawful authority cannot be resolved without state secrets. Plaintiffs
9 allege "that the Program's surveillance has been conducted without Court orders" for several
10 years, and that it involves "the wholesale, long-term interception of customer communications
11 seen here." Pls. Prelim. Inj. Mem. at 20. Plaintiffs also seek to address whether the Government
12 certified to AT&T, pursuant to the statutory provisions on which Plaintiffs have based their
13 claims, the lawfulness of the alleged activities, *see id.* n. 23, and whether AT&T's reliance on
14 any such certification would have been reasonable. *Id.* at 21. And Plaintiffs put at issue (as a
15 general matter) those situations in which warrantless wiretapping may lawfully occur. *Id.* at 20-
16 21. Again quite clearly, Plaintiffs' allegations put at issue the factual basis of the alleged
17 activities.
18
19

20 [REDACTED TEXT]
21

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
3 Assistant Attorney General

4 CARL J. NICHOLS
5 Deputy Assistant Attorney General

6 DOUGLAS N. LETTER
7 Terrorism Litigation Counsel

8 JOSEPH H. HUNT
9 Director, Federal Programs Branch

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

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

24 Attorneys for United States of America

25 DATED: May 12, 2006

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

CERTIFICATE OF SERVICE

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

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

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

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

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

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

s/ Anthony J. Coppolino

EXHIBIT 9

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

12 Attorneys for Intervenor Defendant United States of America

13 UNITED STATES DISTRICT COURT
 14 NORTHERN DISTRICT OF CALIFORNIA
 15

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

19 Plaintiffs,)

20 v.)

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

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

Case No. C-06-0672-VRW

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

TABLE OF CONTENTS

1
2
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

INTRODUCTION 1

ARGUMENT 2

I. *IN CAMERA, EX PARTE* REVIEW OF THE UNITED STATES' SUBMISSIONS
DOES NOT VIOLATE DUE PROCESS. 2

II. PLAINTIFFS ARE NOT ENTITLED TO ACCESS TO THE CLASSIFIED
MATERIALS SUBMITTED *IN CAMERA, EX PARTE*. 8

III. PLAINTIFFS HAVE OFFERED NO VALID REASON FOR THE COURT TO
FOREGO REVIEW OF THE *IN CAMERA, EX PARTE* MATERIALS. 13

CONCLUSION 20

CERTIFICATE OF SERVICE

TABLE OF AUTHORITIES

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

CASES

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1	<i>Guenther v. Comm'r of Internal Revenue,</i> 889 F.2d 882 (9th Cir. 1989)	3, 7
2		
3	<i>Haig v. Agee,</i> 453 U.S. 280 (1981)	3, 5
4	<i>Halkin v. Helms,</i> 598 F.2d 1 (D.C. Cir. 1978)	11, 18
5		
6	<i>Halkin v. Helms,</i> 690 F.2d 977 (D.C. Cir. 1982)	15, 16, 18
7	<i>Hayden v. Nat'l Security Agency,</i> 608 F.2d 1381 (D.C. Cir. 1979)	10
8		
9	<i>Holy Land Found. for Relief & Dev. v. Ashcroft,</i> 333 F.3d 156 (D.C. Cir. 2003), <i>cert. denied</i> , 540 U.S. 1218 (2004)	4
10		
11	<i>In re Sealed Case No. 98-3077,</i> 151 F.3d 1059 (D.C. Cir. 1998)	6
12	<i>In re Under Seal,</i> 945 F.2d 1285 (4th Cir. 1991)	18
13		
14	<i>In re United States,</i> 1 F.3d 1251	10
15	<i>In re United States,</i> 872 F.2d 472 (D.C. Cir. 1989)	18
16		
17	<i>Jifry v. Fed. Aviation Admin.,</i> 370 F.3d 1174 (D.C. Cir. 2004), <i>cert. denied</i> , 543 U.S. 1146 (2005)	3
18		
19	<i>Kasza v. Browner,</i> 133 F.3d 1159 (9th Cir. 1988)	passim
20	<i>Lujan v. Defenders of Wildlife,</i> 504 U.S. 555 (1992)	12, 14
21		
22	<i>Lynn v. Regents of Univ. of Calif.,</i> 656 F.2d 1337 (9th Cir. 1981)	7
23	<i>Meridian Int'l Logistics, Inc. v. United States,</i> 939 F.2d 740 (9th Cir. 1991)	2, 3, 6, 7
24		
25	<i>Molerio v. Fed. Bureau of Investigation,</i> 749 F.2d 815 (D.C. Cir. 1984)	16
26	<i>Morrissey v. Brewer,</i> 408 U.S. 471 (1972)	6
27		

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

2

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

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

5

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

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

8

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

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

11

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

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

14

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

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

17

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

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

20

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

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

23

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

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

26

27

1	<i>United States v. Duggan,</i>	
	743 F.2d 59 (2d Cir. 1984)	12
2		
3	<i>United States v. Hamide,</i>	
	914 F.2d 1147 (9th Cir. 1990)	12
4	<i>United States v. Isa,</i>	
	923 F.2d 1300 (8th Cir. 1991)	12
5		
6	<i>United States v. Johnson,</i>	
	952 F.2d 565 (1st Cir. 1991)	12
7	<i>United States v. Klimavicius-Viloria,</i>	
	144 F.3d 1249 (9th Cir. 1998)	8
8		
9	<i>United States v. Ott,</i>	
	827 F.2d 473 (9th Cir. 1987)	3, 12
10	<i>United States v. Reynolds,</i>	
	345 U.S. 1 (1953)	17
11		
12	<i>United States v. Squillacote,</i>	
	221 F.3d 542 (4th Cir. 2000)	12
13	<i>United States v. Thompson,</i>	
	827 F.2d 1254 (9th Cir. 1987)	8
14		
15	<i>Wayte v. United States,</i>	
	470 U.S. 598 (1985)	
16	<i>Weberman v. Nat'l Security Agency,</i>	
	668 F.2d 676 (2d Cir. 1982)	10
17		

STATUTES

19	Cal. Bus. & Prof. Code §§ 17200, <i>et seq</i>	16
20	18 U.S.C. § 2511	16
21	47 U.S.C. § 605, 18 U.S.C. § 2702	16
22	47 U.S.C. § 2511(2)	17
23	50 U.S.C. § 402	12
24	50 U.S.C. § 1801 <i>et seq</i>	passim
25	50 U.S.C. § 1806(f)	9, 11, 12
26	50 U.S.C. § 1809	16
27		

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

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

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

INTRODUCTION

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

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

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

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

18 **ARGUMENT**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1 construction of a statute would raise serious constitutional problems, and where an alternative
2 interpretation of the statute is 'fairly possible,' we are obligated to construe the statute to avoid
3 such problems.") (quoting *INS v. St. Cyr*, 533 U.S. 289, 299-300 (2001)) (citation omitted). In
4 addition, when Congress intentionally seeks to restrict or regulate presidential action through
5 legislation, it must make that intention clear. See *Armstrong v. Bush*, 924 F.2d 282, 289 (D.C.
6 Cir. 1991) ("[I]n legislation regulating presidential action . . . raises 'serious' practical, political,
7 and constitutional questions that warrant careful congressional and presidential consideration")
8 (citing *United States v. Bass*, 404 U.S. 336, 350 (1971)). Section 1806(f) does not set forth a
9 clear intention to restrict the President's constitutionally-imposed authority to protect and control
10 national security information in the context of this case. See *Egan*, 484 U.S. at 527.

11 **III. PLAINTIFFS HAVE OFFERED NO VALID REASON FOR THE COURT TO**
12 **FOREGO REVIEW OF THE *IN CAMERA*, *EX PARTE* MATERIALS.**

13 Plaintiffs' remaining arguments – that the Court need not review the *in camera*, *ex parte*
14 materials because Plaintiffs can prove their *prima facie* case based on the public record, see Pltfs'
15 Br. at 5-9, that the Court's review of the *in camera*, *ex parte* materials is premature, see *id.* at 10-
16 14, and that it would be appropriate to permit discovery into any certifications AT&T may have
17 received from the United States, see *id.* at 14 – all reflect a fundamental misconception of the
18 scope, nature and effect of the Government's invocation of the state secrets privilege.

19 Although the primary reasons for rejecting Plaintiffs' arguments are set forth in the
20 Government's *in camera*, *ex parte* materials, several arguments that can be made on the public
21 record demonstrate that Plaintiffs' position is without merit. Plaintiffs' primary argument for
22 deferring review of the *in camera*, *ex parte* materials is that they "can sustain their *prima facie*
23 case without resort to the classified materials." Pltfs' Br. at 5. But this argument ignores the
24 well-established rule that if "the 'very subject matter of the action' is a state secret, then the court
25 should dismiss the plaintiff's action based solely on the invocation of the state secrets privilege."
26 *Kasza*, 133 F.3d at 1166 (citing *United States v. Reynolds*, 345 U.S. 1, 11 n.26 (1953)); see also

1 *Totten v. United States*, 92 U.S. 105, 107 (1875) (“[P]ublic policy forbids the maintenance of any
2 suit in a court of justice, the trial of which would inevitably lead to the disclosure of matters
3 which the law itself regards as confidential, and respecting which it will not allow the confidence
4 to be violated.”); *see also Tenet v. Doe*, 544 U.S. 1, 8 (2005) (applying *Totten* to bar a suit
5 brought by former Soviet double agents seeking to enforce their alleged employment agreements
6 with the CIA and making clear that the *Totten* bar applies whenever a party’s “success depends
7 upon the existence of [a] secret espionage relationship with the government”). In such cases, the
8 state secrets are “so central to the subject matter of the litigation that any attempt to proceed will
9 threaten disclosure of the privileged matters.” *Fitzgerald v. Penthouse Int’l, Ltd.*, 776 F.2d 1236,
10 1241-42 (4th Cir. 1985). For the reasons discussed in the Government’s *in camera, ex parte*
11 filing, the very subject matter of Plaintiffs’ allegations is a state secret and further litigation
12 would inevitably risk their disclosure.

13 Even if the very subject matter of Plaintiffs’ allegations were not state secrets, Plaintiffs
14 are wrong to claim that they can make out a *prima facie* claim absent the excluded state secrets.
15 As noted above, in order to prevail on any of their claims, Plaintiffs bear the burden of
16 establishing standing and must, at an “irreducible constitutional minimum,” demonstrate (1) an
17 injury-in-fact, (2) a causal connection between the injury and the conduct complained of, and (3)
18 a likelihood that the injury will be redressed by a favorable decision. *Lujan*, 504 U.S. at 560-61.
19 In meeting that burden, the named Plaintiffs must demonstrate an actual or imminent – not
20 speculative or hypothetical – injury that is particularized as to them; they cannot rely on alleged
21 injuries to unnamed members of a purported class. And to obtain prospective relief, Plaintiffs
22 must show that they are “immediately in danger of sustaining some direct injury” as the result of
23 the challenged conduct. *City of Los Angeles v. Lyons*, 461 U.S. 95, 102 (1983); *O’Shea v.*
24 *Littleton*, 414 U.S. 488, 495-96 (1974).

25 As demonstrated in the Government’s public briefs and declarations, Plaintiffs cannot
26 prove these jurisdictional elements without information covered by the state secrets assertion.

1 The Government’s privilege assertion covers any information that tends to confirm or deny (a)
 2 the alleged intelligence activities, (b) whether AT&T was involved with any such activity, and
 3 (c) whether a particular individual’s communications were intercepted as a result of any such
 4 activity. See Declaration of John D. Negroponte, Director of National Intelligence, U.S. Mem.,
 5 Attachment 1 (“Negroponte Decl.”), ¶¶ 11-12. Without these facts – which must be removed
 6 from the case as a result of the state secrets assertion – Plaintiffs cannot establish any alleged
 7 injury that is fairly traceable to AT&T.⁷ Thus, regardless of whether they adequately allege such
 8 facts, Plaintiffs ultimately will not be able to prove injury-in-fact or causation—and thus cannot
 9 establish this Court’s jurisdiction, let alone sustain a *prima facie* case, without information
 10 subject to the state secrets privilege.⁸

11

12 ⁷ Because jurisdictional issues must be examined as a threshold question, *see, e.g., Steel*
 13 *Co. v. Citizens for a Better Environment*, 523 U.S. 83, 94-95 (1998), if the Court were to
 14 determine on the basis of the public record that Plaintiffs failed to establish their standing
 15 because, for example, Plaintiffs have failed to meet their burden to do so as a matter of law, or
 16 because it is clear from the public record that, in light of United States’ inability to confirm or
 17 deny whether any individual Plaintiff is the subject of surveillance, the Court may find it
 unnecessary to review the United States’ *in camera, ex parte* submissions, and may dismiss this
 case on that ground alone. Otherwise, however, review of the materials submitted *in camera* and
ex parte is necessary to adjudicate the state secrets issues posed by this case. As a result, the
 Court could dismiss this case on the basis of the Government’s public assertion of the state
 secrets privilege.

18 ⁸ As the United States noted in its public brief, to the extent Plaintiffs challenge the
 19 Terrorist Surveillance Program (“TSP”), *see, e.g., Am. Compl.* 32-37, the allegations in the
 20 Complaint are insufficient on their face to establish standing even apart from the state secrets
 21 issue because Plaintiffs fail to demonstrate that they fall anywhere near the scope of that
 22 program. Plaintiffs do not claim to be, or to communicate with, members or affiliates of al
 23 Qaeda – indeed, Plaintiffs expressly *exclude* from their purported class any foreign powers or
 24 agents of foreign powers, “including without limitation anyone who knowingly engages in
 25 sabotage or international terrorism, or activities that are in preparation therefore.” *Am. Compl.*
 26 ¶ 70. The named Plaintiffs thus are in no different position from any other citizen or AT&T
 27 subscriber who falls *outside* the narrow scope of the TSP but nonetheless disagrees with the
 28 program. Such a generalized grievance is clearly insufficient to support either constitutional or
 prudential standing to challenge the TSP. *See Halkin v. Helms*, 690 F.2d 977, 1001-03 (D.C. Cir.
 1982) (“*Halkin II*”) (holding that individuals and organizations opposed to the Vietnam War
 lacked standing to challenge intelligence activities because they did not adequately allege that
 they were (or immediately would be) subject to such activities; thus, their claims were “nothing
 more than a generalized grievance against the intelligence-gathering methods sanctioned by the
 President”) (internal quotation marks and citation omitted); *United Presbyterian Church in the*
U.S.A. v. Reagan, 738 F.2d 1375, 1380 (D.C. Cir. 1984) (rejecting generalized challenge to
 alleged unlawful surveillance). To the extent Plaintiffs allege classified intelligence activities

1 Plaintiffs' inability to sustain a *prima facie* case is not limited to their inability to prove
2 their standing. More generally, as the Government explained in its public brief, adjudicating
3 each claim in the Amended Complaint would require confirmation or denial of the existence,
4 scope, and potential targets of alleged intelligence activities, as well as AT&T's alleged
5 involvement in such activities.⁹ Because such information cannot be confirmed or denied
6 without causing exceptionally grave damage to the national security, Plaintiffs' attempt to make
7 out a *prima facie* case would run into privileged information. Where, as here, a plaintiff cannot
8 make out a *prima facie* case in support of its claims absent the excluded state secrets, the case
9 must be dismissed. See *Kasza*, 133 F.3d at 1166; *Halkin II*, 690 F.2d at 998-99; *Fitzgerald*, 776
10 F.2d at 1240-41.

11 Plaintiffs' argument also fails to recognize that litigation is not limited to determining
12 whether a plaintiff can establish a *prima facie* case. For that very reason, courts have recognized
13 that if the state secrets privilege "deprives the *defendant* of information that would otherwise
14 give the defendant a valid defense to the claim, then the court may grant summary judgment to
15 the defendant." *Kasza*, 133 F.3d at 1166 (quoting *Bareford v. General Dynamics Corp.*, 973
16 F.2d 1138, 1141 (5th Cir. 1992)); see also *Molerio v. Fed. Bureau of Investigation*, 749 F.2d
17 815, 825 (D.C. Cir. 1984) (granting summary judgment where state secrets privilege precluded
18 _____
19 beyond the TSP, Plaintiffs could not prove such allegations in light of the state secrets assertion.

20 ⁹ As the United States demonstrated in its public brief, to prove their FISA claim (as
21 alleged in Count I), Plaintiffs would have to show that AT&T intentionally acquired, under color
22 of law and by means of a surveillance device within the United States, the contents of one or
23 more wire communications to or from Plaintiffs. See Am Compl. ¶¶ 93-94; 50 U.S.C.
24 §§ 1801(f), 1809, 1810. Likewise, to prove their claim under 18 U.S.C. § 2511 (as alleged in
25 Count III), Plaintiffs would have to demonstrate that AT&T intentionally intercepted, disclosed,
26 used, and/or divulged the contents of Plaintiffs' wire or electronic communications. See Am.
27 Compl. ¶¶ 102-07. Plaintiffs' claims under 47 U.S.C. § 605, 18 U.S.C. § 2702, and Cal. Bus. &
28 Prof. Code §§ 17200, *et seq.*, all require similar proof: the acquisition and/or disclosure of
Plaintiffs' communications and related information. And Plaintiffs must also prove, for each of
their statutory claims, that any alleged interception or disclosure was not authorized by the
Government. Despite Plaintiffs' unsupported assumption that they could demonstrate some or
all of these necessary facts on the basis of the public record, the Government's submissions make
clear that any information tending to confirm or deny the alleged activities, or any alleged AT&T
involvement, is subject to the state secrets privilege. See Negroponete Decl. ¶¶ 11-12.

1 the Government from using a valid defense). In this case – as noted in the United States’ public
2 brief and as demonstrated in the *in camera, ex parte* materials – neither AT&T nor the
3 Government could defend this action on the grounds that, among other things, the activities
4 alleged by the Complaint (i) were authorized by the Government; (ii) did not require a warrant
5 under the Fourth Amendment; (iii) were reasonable under the Fourth Amendment; or (iv) were
6 otherwise authorized by law. *See* U.S. Mem. at 14-29.

7 Plaintiffs suggest that the Court could adjudicate whether AT&T received any
8 certification or authorization from the Government relating to the alleged surveillance activity.
9 They are mistaken. The United States has explained that the state secrets assertion “covers any
10 information tending to confirm or deny” whether “AT&T was involved with any” of the “alleged
11 intelligence activities.” *See* U.S. Mem. at 17-18. Clearly, the existence or non-existence of any
12 certification or authorization by the Government relating to any AT&T activity would be
13 information tending to confirm or deny AT&T’s involvement in any alleged intelligence activity.
14 Thus, any such activity would fall within the Government’s state secrets assertion, and the Court
15 could not adjudicate, or allow discovery regarding, whether any Government certification or
16 authorization exists without considering the Government’s assertion of the state secrets privilege.
17 *See id.* at 23.¹⁰

18 Finally, Plaintiffs argue that before the Court can review the *in camera, ex parte*
19 materials, the Government must make a more specific – *i.e.*, public – showing about the
20 information subject to the state secrets privilege. But requiring such a showing would be
21 improper where, as here, it would “force ‘disclosure of the very thing the privilege is designed to
22 protect.’” *Ellsberg v. Mitchell*, 709 F.2d 51, 63 (D.C. Cir. 1983) (quoting *United States v.*
23 *Reynolds*, 345 U.S. 1, 8 (1953)); *see also* 709 F.2d at 63 (noting the Court’s “[f]ear” that “an
24

25 ¹⁰ Plaintiffs argue that 47 U.S.C. § 2511(2)(a)(ii) actually requires discovery of any
26 certifications. That is simply wrong. That provision precludes any entity that has received such
27 a certification from disclosing that certification “except as may otherwise be required by legal
28 process.” *Id.* Moreover, any “legal process” includes the determination of whether any privilege,
including the state secrets privilege or any statutory privilege, prohibits such disclosure.

1 insufficient public justification result in denial of the privilege entirely might induce the
2 government's representatives to reveal some material that, in the interest of national security,
3 ought not to be uncovered"; further noting the "considerable variety in the situations in which a
4 state secrets privilege may be fairly asserted"). As DNI Negroponte states in his Public
5 Declaration, "any further elaboration on the public record concerning these matters [covered by
6 his Declaration] would reveal information that could cause the very harms my assertion of the
7 state secrets privilege is intended to prevent." See Negroponte Decl. ¶¶ 11-12. In light of this
8 determination by the nation's highest-ranking intelligence official, the Government cannot say
9 more publicly, and should not – and cannot – be penalized in this litigation because it has done
10 nothing other than take the steps necessary to protect the national security of the United States.¹¹

11 Not surprisingly, Plaintiffs are unable to point to any state secrets case in which the court
12 has refused to review *in camera*, *ex parte* materials on the ground that the Government had
13 insufficiently described the state secrets on the public record. Instead, *Nixon v. Sirica*, 487 F.2d
14 700 (D.C. Cir. 1973) (*en banc*), on which Plaintiffs rely for the proposition that a more
15 particularized public showing must be made before a court conducts an *in camera* review of
16 privileged materials, is a case that involving the assertion of *executive privilege*, not the state
17 secrets privilege.¹² *Id.* at 715-16.

18
19 ¹¹ See, e.g., *In re United States*, 872 F.2d 472, 476 (D.C. Cir. 1989) ("Notions of
20 sovereign immunity preclude any further adverse consequence to the government, such as
21 alteration of procedural or substantive rules."); *Salisbury*, 690 F.2d at 975 ("when the
22 government is defendant . . . an adverse finding cannot be rendered against it as the price of
asserting an evidentiary privilege"); *Halkin I*, 598 F.2d at 10 (rejecting as "faulty" the premise
"that the defendants should not be permitted to avoid liability for unconstitutional acts by
asserting a privilege which would prevent plaintiffs from proving their case").

23 ¹² The executive privilege, like the state secrets privilege, is constitutionally grounded.
24 The executive privilege, however, protects the President's generalized interest in the
25 confidentiality of his communications, and, as *Nixon* establishes, is a qualified privilege (at least
26 in criminal cases). See 487 F.2d at 716. The state secrets privilege, on the other hand, is a
27 privilege that directly derives from the President's constitutional responsibility to determine,
based on his particular expertise, which disclosures will result in harm to the national security.
Once properly invoked, the state secrets privilege is absolute. *In re Under Seal*, 945 F.2d 1285,
1288 (4th Cir. 1991); see also *Halkin II*, 690 F.2d at 980 ("[S]ecrets of state – matters the
revelation of which reasonably could be seen as a threat to the military or diplomatic interest of

1 Instead, Plaintiffs try to contrast the Government's public filings in this case with the
2 materials filed on the public record in *Kasza v. Browner*, 133 F.3d 1159 (9th Cir. 1998).
3 Although there is no indication in *Kasza* (and no basis in law or logic) to suggest that the Court
4 was creating a minimum requirement for public descriptions of state secrets assertions, in this
5 case the Government has made a similar public showing to that made in *Kasza*. In *Kasza*, the
6 declarant identified categories of information that were validly classified, describing those
7 categories in general terms, such as, for example, "program names"; "missions"; "capabilities";
8 "intelligence sources and methods"; "security sensitive environmental data"; and "military plans,
9 weapons or operations." *Id.* at 1168-69; *see also Edmonds*, 323 F. Supp. 2d at 74 (upholding
10 assertion of state secrets privilege and granting defendant's motion to dismiss where the Attorney
11 General concluded that "further disclosure of the information underlying this case, including the
12 nature of the duties of plaintiff or the other contract translators at issue in this case reasonably
13 could be expected to cause serious damage to the national security interests of the United States"
14 and finding this assertion "similar to the one submitted to the court in *Kasza*").

15 The United States' public filings in this case are no less specific than the public
16 submissions made in *Kasza* and *Edmonds*. For example, DNI Negroponte states in his Public
17 Declaration that to disclose additional details regarding the Terrorist Surveillance Program
18 beyond the facts already disclosed by the President would disclose "classified intelligence
19 information" and reveal "intelligence sources and methods," as a result of which adversaries of
20 the United States would be able "to avoid detection by the U.S. Intelligence Community and/or
21 take measures to defeat or neutralize U.S. intelligence collection, posing a serious threat of
22 damage to the United States' national security interests." Negroponte Decl. ¶ 11; *see also El-*
23 *Masri*, Slip Op. at 10-11 (finding that even where Government had made "a general admission
24 that rendition exists," the Government "validly claimed as state secrets" the "operational details
25 of the extraordinary rendition program"). With respect to Plaintiffs' allegations regarding other

26 _____
27 the nation – are absolutely privileged from disclosure in the courts.”).

1 purported activities of the NSA, including allegations about NSA's purported involvement with
2 AT&T, DNI Negropte further states that the United States can neither confirm nor deny
3 allegations concerning "intelligence activities," "sources," "methods," "relationships," or
4 "targets." Negropte Decl. ¶ 12. And DNI Negropte goes on to note that "disclosure of those
5 who are targeted by such activities would compromise the collection of intelligence information
6 just as disclosure of those who do are not targeted would reveal to adversaries that certain
7 communications channels are secure or, more broadly, would tend to reveal the methods being
8 used to conduct surveillance." *Id.*

9 In sum, where (as here) requiring further public descriptions of the state secrets assertion
10 would "force 'disclosure of the very thing the privilege is designed to protect,'" *Ellsberg*, 709
11 F.2d at 63 (citing *Reynolds*, 345 U.S. at 8), and where (as here) the Government has made a
12 public showing similar to that in *Kasza*, 133 F.3d at 1168-69, there is no reason for the Court to
13 require further public disclosures before reviewing the *in camera*, *ex parte* materials.

14 **CONCLUSION**

15 For the reasons stated herein, the Court should consider the United States' *in camera*, *ex*
16 *parte* submissions and rule on the Government's assertion of the state secrets privilege and its
17 Motion to Dismiss or, in the Alternative, for Summary Judgment before taking any further action
18 in this case.

19 Respectfully submitted,

20 PETER D. KEISLER
Assistant Attorney General, Civil Division

21 CARL J. NICHOLS
Deputy Assistant Attorney General

22 DOUGLAS N. LETTER
Terrorism Litigation Counsel

23 JOSEPH H. HUNT
Director, Federal Programs Branch

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

ANTHONY J. COPPOLINO
Special Litigation Counsel
tony.coppolino@usdoj.gov

s/ Renée S. Orleans

RENÉE S. ORLEANS
renee.orleans@usdoj.gov
ANDREW H. TANNENBAUM
andrew.tannenbaum@usdoj.gov
U.S. Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Avenue, NW
Washington, D.C. 20001
Phone: (202) 514-4782/(202) 514-4263
Fax: (202) 616-8460/(202) 616-8202/(202) 318-2461

DATED: May 24, 2006

Attorneys for Intervenor Defendant United States

CERTIFICATE OF SERVICE

I hereby certify that the foregoing **UNITED STATES' RESPONSE TO PLAINTIFFS' MEMORANDUM OF POINTS AND AUTHORITIES IN RESPONSE TO THE COURT'S MAY 17, 2006 MINUTE ORDER** will be served by means of the Court's CM/ECF system, which will send notifications of such filing to the following:

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

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

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

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

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

s/ Renée S. Orleans

EXHIBIT 10

1 UNITED STATES DISTRICT COURT
2 NORTHERN DISTRICT OF CALIFORNIA

3
4 TASH HEPTING, GREGORY HICKS)
5 CAROLYN JEWEL and ERIK KNUTZEN)
6 on Behalf of Themselves and All Others)
7 Similarly Situated,)

8 Plaintiffs,)

9 v.)

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

12 Defendants.)

Case No. C-06-0672-VRW

**DECLARATION OF
JOHN D. NEGROPONTE,
DIRECTOR OF NATIONAL
INTELLIGENCE**

13 I, John D. Negroponte, declare as follows:

14 **INTRODUCTION**

15 1. I am the Director of National Intelligence (DNI) of the United States. I have held
16 this position since April 21, 2005. From June 28, 2004, until appointed to be DNI, I served as
17 United States Ambassador to Iraq. From September 18, 2001, until my appointment in Iraq, I
18 served as the United States Permanent Representative to the United Nations. I have also served
19 as Ambassador to Honduras (1981-1985), Mexico (1989-1993), the Philippines (1993-1996),
20 and as Deputy Assistant to the President for National Security Affairs (1987-1989).

21 2. In the course of my official duties, I have been advised of this lawsuit and the
22 allegations at issue in this case. The statements made herein are based on my personal
23 knowledge, as well as on information provided to me in my official capacity as DNI, and on my
24 personal evaluation of that information. In personally considering this matter, I have executed a
25 separate classified declaration dated May 12, 2006, and filed *in camera* and *ex parte* in this case.
26 Moreover, I have read and personally considered the information contained in the *In Camera, Ex*
Parte Declaration of Lt. Gen. Keith B. Alexander filed in this case. General Alexander is the

27 DECLARATION OF JOHN D. NEGROPONTE,
28 DIRECTOR OF NATIONAL INTELLIGENCE
Case No. C 06-0672-JCS

1 Director of the National Security Agency (“NSA”), and is responsible for directing the NSA,
2 overseeing the operations undertaken to carry out its mission, and by specific charge from the
3 President and the DNI, protecting NSA activities and intelligence sources and methods.

4 3. The purpose of this declaration is to formally assert, in my capacity as DNI and
5 head of the United States Intelligence Community, the military and state secrets privilege
6 (hereafter “state secrets privilege”), as well as a statutory privilege under the National Security
7 Act, *see* 50 U.S.C. § 403-1(i)(1), in order to protect intelligence information, sources and
8 methods that are implicated by the allegations in this case. Disclosure of the information
9 covered by these privilege assertions reasonably could be expected to cause exceptionally grave
10 damage to the national security of the United States and, therefore, should be excluded from any
11 use in this case. In addition, I concur with General Alexander’s conclusion that the risk is great
12 that further litigation will risk the disclosure of information harmful to the national security of
13 the United States and, accordingly, this case should be dismissed. *See* Declaration of Lt. Gen.
14 Keith B. Alexander, Director, National Security Agency.

15 **BACKGROUND ON DIRECTOR OF NATIONAL INTELLIGENCE**

16 4. The position of Director of National Intelligence was created by Congress in the
17 Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, §§ 1011(a) and
18 1097, 118 Stat. 3638, 3643-63, 3698-99 (2004) (amending sections 102 through 104 of the Title
19 I of the National Security Act of 1947). Subject to the authority, direction, and control of the
20 President, the DNI serves as the head of the U.S. Intelligence Community and as the principal
21 advisor to the President, the National Security Council, and the Homeland Security Council, for
22 intelligence-related matters related to national security. *See* 50 U.S.C. § 403(b)(1), (2).

23 5. The “United States Intelligence Community” includes the Office of the Director
24 of National Intelligence; the Central Intelligence Agency; the National Security Agency; the
25 Defense Intelligence Agency; the National Geospatial-Intelligence Agency; the National
26 Reconnaissance Office; other offices within the Department of Defense for the collection of

27 DECLARATION OF JOHN D. NEGROPONTE,
28 DIRECTOR OF NATIONAL INTELLIGENCE
Case No. C 06-0672-JCS

1 specialized national intelligence through reconnaissance programs; the intelligence elements of
2 the military services, the Federal Bureau of Investigation, the Department of Treasury, the
3 Department of Energy, Drug Enforcement Administration, and the Coast Guard; the Bureau of
4 Intelligence and Research of the Department of State; the elements of the Department of
5 Homeland Security concerned with the analysis of intelligence information; and such other
6 elements of any other department or agency as may be designated by the President, or jointly
7 designated by the DNI and heads of the department or agency concerned, as an element of the
8 Intelligence Community. *See* 50 U.S.C. § 401a(4).

9 6. The responsibilities and authorities of the DNI are set forth in the National
10 Security Act, as amended. *See* 50 U.S.C. § 403-1. These responsibilities include ensuring that
11 national intelligence is provided to the President, the heads of the departments and agencies of
12 the Executive Branch, the Chairman of the Joint Chiefs of Staff and senior military commanders,
13 and the Senate and House of Representatives and committees thereof. 50 U.S.C. § 403-1(a)(1).
14 The DNI is also charged with establishing the objectives of, determining the requirements and
15 priorities for, and managing and directing the tasking, collection, analysis, production, and
16 dissemination of national intelligence by elements of the Intelligence Community. *Id.* § 403-
17 1(f)(1)(A)(i) and (ii). The DNI is also responsible for developing and determining, based on
18 proposals submitted by heads of agencies and departments within the Intelligence Community,
19 an annual consolidated budget for the National Intelligence Program for presentation to the
20 President, and for ensuring the effective execution of the annual budget for intelligence and
21 intelligence-related activities, and for managing and allotting appropriations for the National
22 Intelligence Program. *Id.* § 403-1(c)(1)-(5).

23 7. In addition, the National Security Act of 1947, as amended, provides that "The
24 Director of National Intelligence shall protect intelligence sources and methods from
25 unauthorized disclosure." 50 U.S.C. § 403-1(i)(1). Consistent with this responsibility, the DNI
26 establishes and implements guidelines for the Intelligence Community for the classification of

1 information under applicable law, Executive Orders, or other Presidential directives and access
2 and dissemination of intelligence. *Id.* § 403-1(i)(2)(A), (B). In particular, the DNI is responsible
3 for the establishment of uniform standards and procedures for the grant of access to Sensitive
4 Compartmented Information (“SCI”) to any officer or employee of any agency or department of
5 the United States, and for ensuring consistent implementation of those standards throughout such
6 departments and agencies. *Id.* § 403-1(j)(1), (2).

7 8. By virtue of my position as the DNI, and unless otherwise directed by the
8 President, I have access to all intelligence related to the national security that is collected by any
9 department, agency, or other entity of the United States. Pursuant to Executive Order No.
10 12958, 3 C.F.R. § 333 (1995), as amended by Executive Order 13292 (March 25, 2003),
11 reprinted as amended in 50 U.S.C.A. § 435 at 93 (Supp. 2004), the President has authorized me
12 to exercise original TOP SECRET classification authority. My classified declaration, as well as
13 the classified declaration of General Alexander on which I relied in this case, are properly
14 classified under § 1.3 of Executive Order 12958, as amended, because the public disclosure of
15 the information contained in those declarations could reasonably be expected to cause serious
16 damage to the foreign policy and national security of the United States.

17 **ASSERTION OF THE STATE SECRETS PRIVILEGE**

18 9. After careful and actual personal consideration of the matter, I have determined
19 that the disclosure of certain information implicated by Plaintiffs’ claims—as set forth here and
20 described in more detail in my classified declaration and in the classified declaration of General
21 Alexander—could reasonably be expected to cause exceptionally grave damage to the national
22 security of the United States and, thus, must be protected from disclosure and excluded from this
23 case. Thus, as to this information, I formally invoke and assert the state secrets privilege. In
24 addition, it is my judgment that any attempt to proceed in the case will substantially risk the
25 disclosure of the privileged information described briefly herein, and in more detail in the
26 classified declarations, and will cause exceptionally grave damage to the national security of the

27 DECLARATION OF JOHN D. NEGROPONTE,
28 DIRECTOR OF NATIONAL INTELLIGENCE
Case No. C 06-0672-JCS

1 United States.

2 10. Through this declaration, I also invoke and assert a statutory privilege held by the
3 DNI under the National Security Act to protect intelligence sources and methods implicated by
4 this case. *See* 50 U.S.C. § 403-1(i)(1). My assertion of this statutory privilege for intelligence
5 information and sources and methods is cocxtensive with my state secrets privilege assertion.

6 **INFORMATION SUBJECT TO CLAIMS OF PRIVILEGE**

7 11. In an effort to counter the al Qaeda threat, the President of United States
8 authorized the NSA to utilize its SIGINT capabilities to collect certain "one-end foreign"
9 communications where one party is associated with the al Qaeda terrorist organization for the
10 purpose of detecting and preventing another terrorist attack on the United States. This activity is
11 known as the Terrorist Surveillance Program ("TSP"). To discuss this activity in any greater
12 detail, however, would disclose classified intelligence information and reveal intelligence
13 sources and methods, which would enable adversaries of the United States to avoid detection by
14 the U.S. Intelligence Community and/or take measures to defeat or neutralize U.S. intelligence
15 collection, posing a serious threat of damage to the United States' national security interests.
16 Thus, any further elaboration on the public record concerning the TSP would reveal information
17 that could cause the very harms my assertion of the state secrets privilege is intended to prevent.
18 The classified declaration of General Alexander that I considered in making this privilege
19 assertion, as well as my own separate classified declaration, provide a more detailed explanation
20 of the information at issue and the harms to national security that would result from its
21 disclosure.

22 12. Plaintiffs also make allegations regarding other purported activities of the NSA,
23 including allegations about NSA's purported involvement with AT&T. The United States can
24 neither confirm nor deny allegations concerning intelligence activities, sources, methods,
25 relationships, or targets. For example, disclosure of those who are targeted by such activities
26 would compromise the collection of intelligence information just as disclosure of those who are

27 DECLARATION OF JOHN D. NEGROPONTE,
28 DIRECTOR OF NATIONAL INTELLIGENCE
Case No. C 06-0672-JCS

1 not targeted would reveal to adversaries that certain communications channels are secure or,
2 more broadly, would tend to reveal the methods being used to conduct surveillance. The only
3 recourse for the Intelligence Community and, in this case, for the NSA, is to neither confirm nor
4 deny these sorts of allegations, regardless of whether they are true or false. To say otherwise
5 when challenged in litigation would result in routine exposure of intelligence information,
6 sources, and methods and would severely undermine surveillance activities in general. Thus, as
7 with the other categories of information discussed in this declaration, any further elaboration on
8 the public record concerning these matters would reveal information that could cause the very
9 harms my assertion of the state secrets privilege is intended to prevent. The classified
10 declaration of General Alexander that I considered in making this privilege assertion, as well as
11 my own separate classified declaration, provide a more detailed explanation of the information at
12 issue, the reasons why it is implicated by Plaintiffs' claims, and the harms to national security
13 that would result from its disclosure.

14 **CONCLUSION**

15 13. In sum, I formally invoke and assert the state secrets privilege, as well as a
16 statutory privilege under the National Security Act, to prevent the disclosure of the information
17 detailed in the two classified declarations that are available for the Court's *in camera* and *ex*
18 *parte* review. Moreover, because proceedings in this case risk disclosure of privileged and
19 classified intelligence-related information, I join with General Alexander in respectfully
20 requesting that the Court dismiss this case to stem the harms to the national security of the
21 United States that will occur if it is litigated.

22
23
24
25
26
27 DECLARATION OF JOHN D. NEGROPONTE,
28 DIRECTOR OF NATIONAL INTELLIGENCE
Case No. C 06-0672-JCS

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

I declare under penalty of perjury that the foregoing is true and correct.

DATE: 5/12/2006



JOHN D. NEGROPONTE
Director of National Intelligence

EXHIBIT 11

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

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

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

Plaintiffs,

v.

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

Defendants.

Case No. C-06-0672-VRW

**DECLARATION OF
LIEUTENANT GENERAL
KEITH B. ALEXANDER, DIRECTOR,
NATIONAL SECURITY AGENCY**

I, Keith B. Alexander, declare as follows:

INTRODUCTION

1. I am the Director of the National Security Agency (NSA), an intelligence agency within the Department of Defense. I am responsible for directing the NSA, overseeing the operations undertaken to carry out its mission and, by specific charge of the President and the Director of National Intelligence, protecting NSA activities and intelligence sources and methods. I have been designated an original TOP SECRET classification authority under Executive Order No. 12958, 60 Fed. Reg. 19825 (1995), as amended on March 25, 2003, and Department of Defense Directive No. 5200.1-R, Information Security Program Regulations, 32 C.F.R. § 159a.12 (2000).

2. The purpose of this declaration is to support the assertion of a formal claim of the military and state secrets privilege (hereafter "state secrets privilege"), as well as a statutory privilege, by the Director of National Intelligence (DNI) as the head of the intelligence community. In this declaration, I also assert a statutory privilege with respect to information about NSA activities. For the reasons described below, and in my classified declaration

DECLARATION OF LT. GEN. KEITH B. ALEXANDER,
DIRECTOR, NATIONAL SECURITY AGENCY
Case No. C 06-0672-JCS

1 provided separately to the court for *in camera* and *ex parte* review, the disclosure of the
2 information covered by these privilege assertions would cause exceptionally grave damage to the
3 national security of the United States. The statements made herein, and in my classified
4 declaration, are based on my personal knowledge of NSA operations and on information made
5 available to me as Director of the NSA.

6 **THE NATIONAL SECURITY AGENCY**

7 3. The NSA was established by Presidential Directive in 1952 as a separately
8 organized agency within the Department of Defense. Under Executive Order 12333, § 1.12.(b),
9 as amended, NSA's cryptologic mission includes three functions: (1) to collect, process, and
10 disseminate signals intelligence ("SIGINT") information, of which communications intelligence
11 ("COMINT") is a significant subset, for (a) national foreign intelligence purpose, (b)
12 counterintelligence purposes, and (c) the support of military operations; (2) to conduct
13 information security activities; and (3) to conduct operations security training for the U.S.
14 Government.

15 4. There are two primary reasons for gathering and analyzing intelligence
16 information. The first, and most important, is to gain information required to direct U.S.
17 resources as necessary to counter external threats. The second reason is to obtain information
18 necessary to the formulation of the United States' foreign policy. Foreign intelligence
19 information provided by NSA is thus relevant to a wide range of important issues, including
20 military order of battle; threat warnings and readiness; arms proliferation; terrorism; and foreign
21 aspects of international narcotics trafficking.

22 5. In the course of my official duties, I have been advised of this litigation and
23 reviewed the allegations in Plaintiffs' Amended Complaint and Motion for a Preliminary
24 Injunction. As described herein and in my separate classified declaration, information
25 implicated by Plaintiffs' claims is subject to the state secrets privilege assertion in this case by
26 the DNI. The disclosure of this information reasonably could be expected to cause exceptionally

27 DECLARATION OF LT. GEN. KEITH B. ALEXANDER,
28 DIRECTOR, NATIONAL SECURITY AGENCY
Case No. C 06-0672-JCS

1 grave damage to the national security of the United States. In addition, it is my judgment that
2 any attempt to proceed in the case will substantially risk disclosure of the privileged information
3 and will cause exceptionally grave damage to the national security of the United States.

4 6. Through this declaration, I also hereby invoke and assert NSA's statutory
5 privilege to protect information related to NSA activities described below and in more detail in
6 my classified declaration. NSA's statutory privilege is set forth in section 6 of the National
7 Security Agency Act of 1959 (NSA Act), Public Law No. 86-36 (codified as a note to 50 U.S.C.
8 § 402). Section 6 of the NSA Act provides that "[n]othing in this Act or any other law . . . shall
9 be construed to require the disclosure of the organization or any function of the National
10 Security Agency [or] any information with respect to the activities thereof. . . ." By this
11 language, Congress expressed its determination that disclosure of any information relating to
12 NSA activities is potentially harmful. Section 6 states unequivocally that, notwithstanding
13 any other law, NSA cannot be compelled to disclose any information with respect to its
14 authorities. Further, NSA is not required to demonstrate specific harm to national security when
15 invoking this statutory privilege, but only to show that the information relates to its activities.
16 Thus, to invoke this privilege, NSA must demonstrate only that the information to be protected
17 falls within the scope of section 6. NSA's functions and activities are therefore protected from
18 disclosure regardless of whether or not the information is classified.

19 **INFORMATION SUBJECT TO CLAIMS OF PRIVILEGE**

20 7. Following the attacks of September 11, 2001, the President of United States
21 authorized the NSA to utilize its SIGINT capabilities to collect certain "one-end foreign"
22 communications where one party is associated with the al Qaeda terrorist organization under the
23 Terrorist Surveillance Program (TSP) for the purpose of detecting and preventing another
24 terrorist attack on the United States. Any further elaboration on the public record concerning the
25 TSP would reveal information that could cause the very harms that the DNI's assertion of the
26 state secrets privilege is intended to prevent. My separate classified declaration provides a more

27 DECLARATION OF LT. GEN. KEITH B. ALEXANDER,
28 DIRECTOR, NATIONAL SECURITY AGENCY
Case No. C 06-0672-JCS

1 detailed explanation of the information at issue and the harms to national security that would
2 result from its disclosure.

3 8. Plaintiffs also make allegations regarding other purported activities of the NSA,
4 including allegations about the NSA's purported involvement with AT&T. Regardless of
5 whether these allegations are accurate or not, the United States can neither confirm nor deny
6 alleged NSA activities, relationships, or targets. To do otherwise when challenged in litigation
7 would result in the exposure of intelligence information, sources, and methods and would
8 severely undermine surveillance activities in general. For example, if the United States denied
9 allegations about intelligence targets in cases where such allegations were false, but remained
10 silent in cases where the allegations were accurate, it would tend to reveal that the individuals in
11 the latter cases were targets. Any further elaboration on the public record concerning these
12 matters would reveal information that could cause the very harms that the DNI's assertion of the
13 state secrets privilege is intended to prevent. My separate classified declaration provides a more
14 detailed explanation of the information at issue and the harms to national security that would
15 result from its disclosure.

16 **CONCLUSION**

17 9. In sum, I support the DNI's assertion of the state secrets privilege and statutory
18 privilege to prevent the disclosure of the information detailed in my classified declaration that is
19 available for the Court's *in camera* and *ex parte* review. I also assert a statutory privilege with
20 respect to information about NSA activities. Moreover, because proceedings in this case risk
21 disclosure of privileged and classified intelligence-related information, I respectfully request that
22 the Court not only protect that information from disclosure, but also dismiss this case to stem the
23 harms to the national security of the United States that will occur if it is litigated.

24
25
26
27 DECLARATION OF I.T. GEN. KEITH B. ALEXANDER,
28 DIRECTOR, NATIONAL SECURITY AGENCY
Case No. C 06-0672-JCS

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

I declare under penalty of perjury that the foregoing is true and correct.

DATE: 12 May 06



LT. GEN. KEITH B. ALEXANDER
Director, National Security Agency

DECLARATION OF LT. GEN. KEITH B. ALEXANDER,
DIRECTOR, NATIONAL SECURITY AGENCY
Case No. C 06-0672-JCS

EXHIBIT 12



OFFICE OF
THE CHAIRMAN

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

May 22, 2006

The Honorable Edward J. Markey
Ranking Member
Subcommittee on Telecommunications and the Internet
Energy and Commerce Committee
U.S. House of Representatives
2108 Rayburn House Office Building
Washington, D.C. 20515

Dear Congressman Markey:

Thank you for your letter regarding recent media reports concerning the collection of telephone records by the National Security Agency. In your letter, you note that section 222 of the Communications Act provides that "[e]very telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to . . . customers." 47 U.S.C. § 222(a). You have asked me to explain the Commission's plan "for investigating and resolving these alleged violations of consumer privacy."

I know that all of the members of this Commission take very seriously our charge to faithfully implement the nation's laws, including our authority to investigate potential violations of the Communications Act. In this case, however, the classified nature of the NSA's activities makes us unable to investigate the alleged violations discussed in your letter at this time.

The activities mentioned in your letter are currently the subject of an action filed in the United States District Court for the Northern District of California. The plaintiffs in that case allege that the NSA has "arrang[ed] with some of the nation's largest telecommunications companies . . . to gain direct access to . . . those companies' records pertaining to the communications they transmit." *Hepting v. AT&T Corp.*, No. C-06-0672-VRW (N.D. Cal.), Amended Complaint ¶ 41 (Feb. 22, 2006). According to the complaint, for example, AT&T Corp. has provided the government "with direct access to the contents" of databases containing "personally identifiable customary proprietary network information (CPNI)," including "records of nearly every telephone communication carried over its domestic network since approximately 2001, records that include the originating and terminating telephone numbers and the time and length for each call." *Id.* ¶¶ 55, 56, 61; *see also, e.g.*, Leslie Cauley, "NSA Has Massive Database of Americans' Phone Calls," *USA Today* A1 (May 11, 2006) (alleging that the NSA "has been secretly collecting the phone call records of tens of millions of Americans, using data provided" by major telecommunications carriers).

The government has moved to dismiss the action on the basis of the military and state secrets privilege. See *Hepting*, Motion to Dismiss or, in the Alternative, for Summary Judgment by the United States of America (May 12, 2006). Its motion is accompanied by declarations from John D. Negroponte, Director of National Intelligence, and Lieutenant General Keith B. Alexander, Director, National Security Agency, who have maintained that disclosure of information “implicated by Plaintiffs’ claims . . . could reasonably be expected to cause exceptionally grave damage to the national security of the United States.” Negroponte Decl. ¶ 9. They specifically address “the NSA’s purported involvement” with specific telephone companies, noting that “the United States can neither confirm nor deny alleged NSA activities, relationships, or targets,” because “[t]o do otherwise when challenged in litigation would result in the exposure of intelligence information, sources, and methods and would severely undermine surveillance activities in general.” Alexander Decl. ¶ 8.

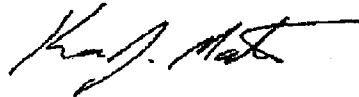
The representations of Director Negroponte and General Alexander make clear that it would not be possible for us to investigate the activities addressed in your letter without examining highly sensitive classified information. The Commission has no power to order the production of classified information. Rather, the Supreme Court has held that “the protection of classified information must be committed to the broad discretion of the agency responsible, and this must include broad discretion to determine who may have access to it. Certainly, it is not reasonably possible for an outside nonexpert body to review the substance of such a judgment.” *Department of the Navy v. Egan*, 484 U.S. 518, 529 (1988).

The statutory privilege applicable to NSA activities also effectively prohibits any investigation by the Commission. The National Security Act of 1959 provides that “nothing in this Act or any other law . . . shall be construed to require the disclosure of the organization or any function of the National Security Agency [or] of any information with respect to the activities thereof.” Pub. L. No. 86-36, § 6(a), 73 Stat. 63, 64, codified at 50 U.S.C. § 402 note. As the United States Court of Appeals for the District of Columbia Circuit has explained, the statute’s “explicit reference to ‘any other law’ . . . must be construed to prohibit the disclosure of information relating to NSA’s functions and activities as well as its personnel.” *Linder v. NSA*, 94 F.3d 693, 696 (D.C. Cir. 1996); see also *Hayden v. NSA/Central Sec. Serv.*, 608 F.2d 1381, 1390 (D.C. Cir. 1979) (“Congress has already, in enacting the statute, decided that disclosure of NSA activities is potentially harmful.”). This statute displaces any authority that the Commission might otherwise have to compel, at this time, the production of information relating to the activities discussed in your letter.

Page 3—The Honorable Edward J. Markey

I appreciate your interest in this important matter. Please do not hesitate to contact me if you have further questions.

Sincerely,

A handwritten signature in black ink, appearing to read "Kevin J. Martin". The signature is fluid and cursive, with a long horizontal stroke at the end.

Kevin J. Martin
Chairman

EXHIBIT 13



THOMAS J. VILBACK, GOVERNOR
SALLY J. PEDERSON, LT. GOVERNOR

JOHN R. NORRIS, CHAIRMAN
DIANE MUNNS, BOARD MEMBER
CURTIS W. SYAMP, BOARD MEMBER

May 25, 2006

Frank Bumette
802 Insurance Exchange Building
505 Fifth Avenue
Des Moines, Iowa 50309-2317

Dear Mr. Bumette:

I am in receipt of your letter of May 22, 2006, asking the Iowa Utilities Board to investigate the actions of AT&T and Verizon Cellular with respect to allegations that those companies, and others, have provided the National Security Agency with access to certain information. Unfortunately, the Board does not have jurisdiction to conduct such an investigation; the services you describe are deregulated in Iowa.

Specifically, Iowa Code § 476.1D requires that the Board deregulate communications services that are subject to effective competition. Pursuant to that statutory duty, the Board has deregulated the long distance services provided by AT&T and the mobile communications services provided by Verizon. Long distance was deregulated in two steps, in 1989 and 1996, and mobile telephone service was deregulated in 1986.

When services are deregulated, "the jurisdiction of the board as to the regulation of [those] communications services is not applicable..." (Iowa Code § 476.1D(1).) Thus, the Board does not have jurisdiction to conduct the investigation you request.

I hope you find this information helpful. If you have any comments or questions concerning this matter, please feel free to contact me at my direct number, 515-281-8272, or by email at david.lynnch@iub.state.ia.us.

Sincerely,

A handwritten signature in black ink, appearing to read "David J. Lynch".

David J. Lynch
General Counsel

Cc:
Iowa Civil Liberties Union
Qwest Corporation

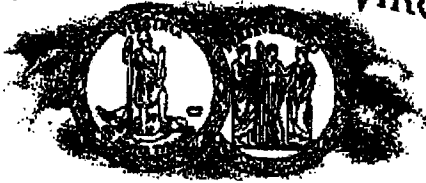
350 MAPLE STREET / DES MOINES, IOWA 50319-0089 / 515.261.5979 / FAX 515.281.5320
[HTTP://WWW.STATE.IA.US/IUR](http://www.state.ia.us/iur)

To see what state Government is accomplishing for Iowans, go to: www.resultsiowa.org

EXHIBIT 14

OFFICE OF THE GENERAL COUNSEL
P.O. Box 1197
Richmond, Virginia 23218-1197

COMMONWEALTH OF VIRGINIA



Telephone Number (804) 371-9671
Facsimile Number (804) 371-9240
Facsimile Number (804) 371-9549

STATE CORPORATION COMMISSION

June 22, 2006

ACLU of Virginia
530 East Main Street
Suite 310
Richmond, Virginia 23219

STATE CORPORATION COMMISSION
RECEIVED
JUN 23 2006
DIVISION OF COMMUNICATIONS
RICHMOND, VA

ATTN: Kent Willis
Executive Director

Rebecca K. Glenberg
Legal Director

RE: Letter complaint dated June 15, 2006

Dear Mr. Willis and Ms. Glenberg:

Your letter complaint dated June 15, 2006, which reiterates your previous request of May 24, 2006, that the State Corporation Commission ("Commission") undertake an investigation of "Verizon," citing a press story in the May 11, 2006, edition of *USA Today* as a basis, has been received and reviewed. However, as before, the June 15 letter complaint identifies no provision of Virginia law, nor any rule or regulation *administered by or under the jurisdiction of the Commission*, which Verizon is alleged to have violated. In addition, your letter does not identify actions that the Commission can take – within its jurisdiction – to resolve the matters raised in your letter, and, as before, I remain unaware of any action the Commission could undertake to resolve these matters.

Your letter and accompanying petition urges the Commission to "investigate these allegations, pursuant to its broad power under Virginia Code § 12.1-12 to 'administer[] the laws made for the regulation and control of corporations doing business in this Commonwealth,' such as the Virginia Consumer Protection Act, and to 'regulat[e] the . . . services . . . of all public service companies.'" (Emphasis added.) However, the Commission is given no authority to conduct any investigation by virtue of the Virginia Consumer Protection Act (the "Act"). Nothing in the Act authorizes any action whatsoever on the part of the Commission.¹

¹ See, §§ 59.1-201 and -201.1 of the Code of Virginia.

Kent Willis, Executive Director
Rebecca K. Glenberg, Legal Director
June 22, 2006
Page 2

Therefore, on my advice, the Commission's Staff continues to decline to initiate the requested investigation.

Very truly,


William H. Chambliss
General Counsel

WHC:sbm

cc: ✓ William Irby

EXHIBIT 15

STATE OF NEW YORK DEPARTMENT OF PUBLIC SERVICE
THREE EMPIRE STATE PLAZA, ALBANY, NY 12223-1350
Internet Address: <http://www.dps.state.ny.us>

PUBLIC SERVICE COMMISSION

WILLIAM M. FLYNN
Chairman
THOMAS J. DUNLEAVY
LEONARD A. WEISS
NEAL N. GALVIN
PATRICIA L. AGAMPORA



DAWN JABLONSKI RYMAN
General Counsel

JAGLYN A. BRILLING
Secretary

June 14, 2006

Donna Lieberman, Executive Director
Corey Stoughton, Staff Attorney
New York Civil Liberties Union
125 Broad Street
New York, New York 10004

Re: New York Civil Liberties Union's Complaint and Request for Investigation
of AT&T and Verizon.

Dear Ms. Lieberman & Mr. Stoughton:

Please accept this letter as my formal response to your correspondence regarding the recent media reports of the alleged cooperation of AT&T and Verizon with the National Security Agency, as well as the Federal Communications Commission's (FCC) actions with respect thereto. As an initial matter, I note that the Public Service Commission of the State of New York takes very seriously the commitment made by the utilities under its jurisdiction to protect the privacy of their customers. In this matter, however, I must inform you that the New York State Public Service Commission respectfully declines to initiate any investigation into the alleged cooperation of AT&T and Verizon with the National Security Agency.

As you may be aware, there is no provision in New York State's Public Service Law specifically concerning the privacy of customer information. Additionally, the existing rules and regulations of the New York State Department of Public Service do not cover activities such as those alleged to have occurred in the recent media reports. On March 22, 1991, in Case 90-C-0075, the Commission released its Statement of Policy on Privacy in Telecommunications. Although that Statement of Policy guides our decisions with respect to our role in overseeing the telecommunication companies under our jurisdiction, the policy statements contained therein do not have the force of law behind them, and, therefore, do not provide this Commission with any authority with which to pursue this matter.

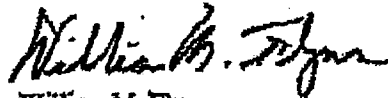
Moreover, in declining to conduct an investigation similar to the one requested in your correspondence, the FCC relied on pleadings submitted by the United States of America in the case of *Hepting v. AT&T*, No. C-06-0672 -- VRW (N.D. Cal.). There, the United States asserted

that the "state secrets" privilege applies to any information connected to this matter. The FCC noted that the same privilege would prevent it from ordering the production of classified information or from compelling any parties which they might investigate to respond to their inquiries. Likewise, the Public Service Commission does not have the authority to compel the production of privileged information, nor does it have the jurisdiction required to pass on questions of law surrounding the assertion of such privilege by the United States, Verizon or AT&T. Accordingly, the Public Service Commission is not the correct agency or government entity to conduct the investigation sought in your correspondence.

Finally, even were the Court to decide that the United States is not entitled to the privilege asserted in the *Hepting* case, the Public Service Commission still is not the correct entity to pursue these matters because of their highly sensitive nature and their connection to national security. Therefore, even were such privilege not to apply, the Public Service Commission would still respectfully decline to initiate the investigation you seek.

I thank you again for your correspondence bringing this matter to our attention. Please feel free to contact me in the future if you have any additional concerns as they relate to the New York State Public Service Commission.

Sincerely,



William M. Flynn
Chairman

cc: Kevin Martin, Chairman, Federal Communications Commission
Ivan Seidenberg, Chairman & CEO, Verizon
William Bair, Executive Vice President & General Counsel, Verizon
Edward Whitacre, Chairman, AT&T
Randall Stephenson, Chief Operating Officer, AT&T
Keefe B. Clemens, Associate General Counsel - NY & CT, Verizon

EXHIBIT 16

KENNY C. GUINN
Governor

STATE OF NEVADA
PUBLIC UTILITIES COMMISSION OF NEVADA
1150 E. William Street
Carson City, Nevada 89701-3109
Policy (775) 684-6107 • Fax (775) 684-6110
Staff (775) 684-6101 • Fax (775) 684-6120
<http://puc.state.nv.us>

received
07/19/06 *JK*
OND

RURAL NEVADA
557 W. Silver Street, No. 207
Elko, Nevada 89801
(775) 738-4914 • Fax (775) 778-6828



SOUTHERN NEVADA OFFICE
101 Convention Center Drive, Suite 250
Las Vegas, Nevada 89109
(702) 486-2600 • Fax (702) 486-2595

July 18, 2006

American Civil Liberties Union of Nevada
Attn: Gary Peck
Assistant General Counsel
732 S. GTS St.
Las Vegas, NV 89101

Re: ACLU vs. AT&T

File: CCU-052606-01 AA

Dear Mr. Peck:

Thank you for your recent communication with the Consumer Complaint Division of the Public Utilities Commission. You submitted consumer complaints against AT&T and Cellco Partnership, Sacramento Valley Limited Partnership, and Southwestco Wireless Limited Partnership (collectively "Verizon Wireless"), which have been assigned our File Nos. CCU-052606-01-AA and CCU-052606-02-AA, respectively. Your complaints were forwarded to these companies for their consideration and response. The Consumer Division received the companies' responses approximately 2 weeks ago. We have reviewed and analyzed these responses to assess the validity of your complaint and any appropriate follow-on action. Primarily because of the legal nature of the responses, the Commission's legal counsel has also been involved in reviewing your complaints and the companies' responses.

As you and the companies have observed, the issues regarding the companies' possible disclosure of call records to agencies of the United States government arose upon publication of national news stories. In their responses, the companies uniformly cite the federally based legal restriction against disclosing whether they did or did not provide customer calling information. They contend that the Public Utilities Commission of Nevada has essentially been preempted by federal law in these matters.

CONSUMER DIVISION:

Carson City/Reno—(775) 684-6100 • Las Vegas—(702) 486-2600 • Other Areas—800-992-0900, Ext. 684-6100

ACLU

Tuesday, July 18, 2006

Page 2 of 3

The overall issue of any disclosure of telecommunications records is being litigated vigorously in lawsuits in various federal courts. At the core of these lawsuits is the legality of the National Security Agency's surveillance program centered in national counterterrorism and security powers and concerns. None of those lawsuits have been finally decided. In these various matters, the United States Dept. of Justice has intervened or actually initiated actions arguing that the state secrets privilege and national security interests preclude disclosure of any responsive measures or actions by the telecommunications companies to any of the federal government's requests.

The United States Department of Justice has notified Verizon, as well as several other carriers, that divulging information even pursuant to a subpoena would be inconsistent with and preempted by federal law. Consequently, Verizon takes the position that it is prohibited from providing any information concerning its alleged cooperation with any National Security Agency program. A person who divulges classified information "concerning the communication intelligence activities of the United States" to any person not authorized by the President or his lawful designee to receive such information would commit a felony. See 18 U. S. C. § 798.

Similarly, in the case of AT&T, the United States Department of Justice has invoked the state secrets privilege and asserted that any claims that AT&T has violated the law through its alleged cooperation with any NSA program "cannot be litigated because adjudication of Plaintiffs' claims would put at risk the disclosure of privileged national security information." 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, filed on May 13, 2006, in *Hepting v. AT&T*, No. C-06-0672-VRW (N.D. Cal.)

Clearly, the United States government is strongly asserting the position that any actions it has taken in requesting information from any telecommunications provider is lawful and disclosure is prohibited. The companies respond that at a minimum the Public Utilities Commission of Nevada cannot go forward with your complaints until there are rulings issued in the appropriate venues concerning these matters and the claims of national security. They assert that they must continue to decline to respond to inquiries as to the release of information to the United States government under the current circumstances. We also note that the United States Congress has the opportunity to scrutinize the assertion of the United States national security and any use of the state secrets law.

We are attaching hereto AT&T's responses to your complaints in which they outline in some detail the foregoing positions. They also attached as part of their responses many of the court related documents cited in their responses but we have not attached those because of the volume of those attachments; you may review them at our offices at your convenience.

We also point out that the Public Utilities Commission of Nevada does not regulate commercial mobile radio service providers (wireless or cell phone service providers) as public utilities. Nevada's regulation of cell phone service providers is limited to the requirement of completion of a registration form and payment of an annual fee. See Nevada Revised Statute 704.033(6), Nevada Administrative Code 704.68026, 704.786-704.7864.

ACLU

Tuesday, July 18, 2006

Page 3 of 3

Additionally, the Public Utilities Commission of Nevada does not regulate long distance providers (telecommunications services to/from other states). The Federal Communications Commission has declined to undertake the investigation of any disclosure of calling information to agencies of the United States government.

Also, as Verizon points out, it does not maintain records of local phone calls. It is this provision of local, wired telephone service that is the subject of rate and service regulation by the Public Utilities Commission of Nevada.

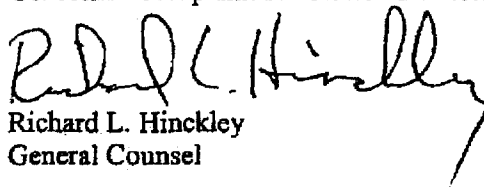
Lastly, NRS 200.630(2) (d) provides that a local telecommunications company and its representatives are not prohibited from disclosing communications when such is done 'on written demand of ...lawful authority.'

We appreciate your concerns with the issues raised, and will continue to monitor the various actions to keep abreast of what is being decided on these important matters. However, based on your complaints, the companies' responses and our review of the responses, we do not find a basis for further action at this time. Thank you for contacting the Commission and sharing your concern.

Sincerely,



Rick Hackman, Manager
Consumer Complaint Resolution Division



Richard L. Hinckley
General Counsel

Cc: Dan Foley, AT&T