

No. 06-17132

**IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT**

TASH HEPTING, *et al.*,

Plaintiffs-Appellees,

v.

AT&T CORP.,

Defendant-Appellant.

On Appeal from the United States District Court
for the Northern District of California

BRIEF OF APPELLANT AT&T CORP.

David W. Carpenter
Bradford A. Berenson
Edward R. McNicholas
Eric A. Shumsky
SIDLEY AUSTIN LLP
1501 K Street, N.W.
Washington, D.C. 20005
(202) 736-8000

Michael K. Kellogg*
Sean A. Lev
KELLOGG, HUBER, HANSEN,
TODD, EVANS & FIGEL, P.L.L.C.
1615 M Street, N.W., Suite 400
Washington, D.C. 20036
(202) 326-7900

Bruce A. Ericson
Kevin M. Fong
Marc H. Axelbaum
Jacob R. Sorensen
PILLSBURY WINTHROP SHAW PITTMAN LLP
50 Fremont Street
San Francisco, CA 94105
(415) 983-1000

March 9, 2007

*Counsel of Record

Counsel for Defendant-Appellant AT&T Corp.

CORPORATE DISCLOSURE STATEMENT

AT&T Corp. is a New York corporation with its principal place of business in New Jersey. It is a wholly owned subsidiary of AT&T Inc., a publicly traded company. No entity owns more than 10% of AT&T Inc. stock.

TABLE OF CONTENTS

	Page
CORPORATE DISCLOSURE STATEMENT	i
TABLE OF AUTHORITIES	iv
PRELIMINARY STATEMENT.....	1
JURISDICTION.....	3
ISSUE PRESENTED FOR REVIEW.....	3
STATEMENT OF THE CASE.....	4
STATEMENT OF FACTS	6
A. Plaintiffs’ Allegations.....	6
1. The TSP.....	7
2. Untargeted Content Surveillance	9
3. Communications Records	11
B. The United States’ and AT&T’s Motions To Dismiss.....	12
C. The District Court’s Decision.....	14
SUMMARY OF ARGUMENT	18
STANDARD OF REVIEW	22
ARGUMENT	22
I. LITIGATION MUST BE DISMISSED WHEN THE STATE SECRETS DOCTRINE PRECLUDES THE PARTIES FROM FULLY AND FAIRLY LITIGATING THE THRESHOLD ISSUE OF STANDING.....	22
A. Plaintiffs Must Prove That They Were Subjected to the Alleged Surveillance and That AT&T Assisted in That Activity	22

B.	When the State Secrets Privilege Prevents the Full and Fair Litigation of Standing, Dismissal Is Required	26
II.	PLAINTIFFS CANNOT ESTABLISH STANDING BECAUSE THE STATE SECRETS PRIVILEGE PRECLUDES ADJUDICATION OF WHETHER AT&T PARTICIPATED IN THE ALLEGED SURVEILLANCE ACTIVITIES.....	31
A.	To Establish Standing, Plaintiffs Must Show That AT&T Participated in the Alleged Surveillance Activities, a Fact That Is Central to the Director of National Intelligence’s State Secrets Assertion	31
B.	The District Court Erred in Hypothesizing That AT&T Must Have Participated in the Alleged Programs	34
III.	PLAINTIFFS CANNOT ESTABLISH STANDING BECAUSE THE STATE SECRETS PRIVILEGE PRECLUDES ADJUDICATION OF WHETHER PLAINTIFFS WERE INJURED BY THE ALLEGED SURVEILLANCE ACTIVITIES	44
A.	The State Secrets Privilege Prevents Adjudication of Whether Plaintiffs Were Injured by Alleged Content Surveillance.....	44
1.	The Allegations of the Complaint Are Insufficient To Establish Standing.....	47
2.	The Marcus and Klein Declarations Are Insufficient To Establish Standing, and Their Validity Cannot Be Litigated Without Violating the State Secrets Privilege.....	49
3.	In Light of the State Secrets Privilege, Discovery Is Not Available	53
B.	The State Secrets Privilege Prevents Adjudication of Whether Plaintiffs Were Injured by the Alleged Records Program	55
	CONCLUSION	59
	STATEMENT OF RELATED CASES	60

TABLE OF AUTHORITIES

Page

Cases

<i>Al-Haramain Islamic Found., Inc. v. Bush</i> , 451 F. Supp. 2d 1215 (D. Or. 2006)	5
<i>ACLU v. Brown</i> , 619 F.2d 1170 (7th Cir. 1980).....	32
<i>ACLU v. NSA</i> , 438 F. Supp. 2d 754 (E.D. Mich. 2006)	56
<i>ASARCO v. Kadish</i> , 490 U.S. 605 (1989)	39, 50
<i>Bareford v. General Dynamics Corp.</i> , 973 F.2d 1138 (5th Cir. 1992).....	27
<i>Casey v. Lewis</i> , 4 F.3d 1516 (9th Cir. 1993).....	23
<i>DaimlerChrysler Corp. v. Cuno</i> , 126 S. Ct. 1854 (2006).....	38, 50, 56, 57
<i>Dreier v. United States</i> , 106 F.3d 844 (9th Cir. 1997)	24
<i>El-Masri v. United States</i> , No. 06-1667, 2007 WL 625130 (4th Cir. Mar. 2, 2007).....	<i>passim</i>
<i>Ellsberg v. Mitchell</i> , 709 F.2d 51 (D.C. Cir. 1983)	14, 25, 26, 27, 29
<i>Farnsworth Cannon, Inc. v. Grimes</i> , 635 F.2d 268 (4th Cir. 1980)	27, 28, 29
<i>Fitzgerald v. Penthouse Int'l, Ltd.</i> , 776 F.2d 1236 (4th Cir. 1985).....	27
<i>Fitzgibbon v. CIA</i> , 911 F.2d 755 (D.C. Cir. 1990)	32
<i>Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC) Inc.</i> , 528 U.S. 167 (2000).....	58
<i>Halkin v. Helms</i> :	
598 F.2d 1 (D.C. Cir. 1978) (“ <i>Halkin I</i> ”)	<i>passim</i>

690 F.2d 977 (D.C. Cir. 1982) (“ <i>Halkin II</i> ”).....	<i>passim</i>
<i>Hayden v. NSA</i> , 608 F.2d 1381 (D.C. Cir. 1979).....	38
<i>Kasza v. Browner</i> , 133 F.3d 1159 (9th Cir. 1998).....	<i>passim</i>
<i>King County v. Rasmussen</i> , 299 F.3d 1077 (9th Cir. 2002)	22
<i>Kowalski v. Tesmer</i> , 543 U.S. 125 (2004)	23
<i>Laird v. Tatum</i> , 408 U.S. 1 (1972).....	24
<i>Lindsey v. Normet</i> , 405 U.S. 56 (1972).....	28
<i>Lujan v. Defenders of Wildlife</i> , 504 U.S. 555 (1992)	23, 24, 49
<i>Martin v. Morgan Drive Away, Inc.</i> , 665 F.2d 598 (5th Cir. 1982)	24
<i>McDonnell Douglas Corp. v. United States</i> :	
37 Fed. Cl. 270 (1996).....	52
323 F.3d 1006 (Fed. Cir. 2003)	27
<i>Molerio v. FBI</i> , 749 F.2d 815 (D.C. Cir. 1984)	27
<i>Philip Morris USA v. Williams</i> , 127 S. Ct. 1057 (2007).....	28
<i>Pony v. County of Los Angeles</i> , 433 F.3d 1138 (9th Cir.), <i>cert. denied</i> , 126 S. Ct. 2864 (2006).....	23
<i>St. Clair v. City of Chico</i> , 880 F.2d 199 (9th Cir. 1989).....	24
<i>Scott v. Pasadena Unified Sch. Dist.</i> , 306 F.3d 646 (9th Cir. 2002)	49
<i>Simon v. Eastern Ky. Welfare Rights Org.</i> , 426 U.S. 26 (1976).....	23
<i>Smelt v. County of Orange</i> , 447 F.3d 673 (9th Cir.), <i>cert. denied</i> , 127 S. Ct. 396 (2006).....	23

<i>Southern Pac. Transp. Co. v. City of Los Angeles</i> , 922 F.2d 498 (9th Cir. 1990)	58
<i>Steel Co. v. Citizens for a Better Env't</i> , 523 U.S. 83 (1998)	58
<i>Sterling v. Tenet</i> , 416 F.3d 338 (4th Cir. 2005), <i>cert. denied</i> , 126 S. Ct. 1052 (2006).....	27, 32
<i>Tenet v. Doe</i> , 544 U.S. 1 (2005).....	3, 32, 43
<i>Terkel v. AT&T Corp.</i> , 441 F. Supp. 2d 899 (N.D. Ill. 2006).....	5, 48, 56
<i>Tooley v. Bush</i> , No. 06-306, 2006 U.S. Dist. LEXIS 92274 (D.D.C. Dec. 21, 2006)	25
<i>Totten v. United States</i> , 92 U.S. 105 (1875)	3, 37, 43
<i>United Presbyterian Church v. Reagan</i> , 738 F.2d 1375 (D.C. Cir. 1984)	25, 50
<i>United States, In re</i> , 872 F.2d 472, 474 (D.C. Cir. 1989).....	26
<i>United States v. Faulkner</i> , 439 F.3d 1221 (10th Cir. 2006)	25
<i>United States v. Ott</i> , 637 F. Supp. 62 (E.D. Cal. 1986), <i>aff'd</i> , 827 F.2d 473 (9th Cir. 1987).....	25
<i>United States v. Reynolds</i> , 345 U.S. 1 (1952).....	26, 35, 42, 50
<i>Valley Forge Christian Coll. v. Americans United for Separation of Church & State, Inc.</i> , 454 U.S. 464 (1982)	23
<i>Vinci v. Waste Mgmt., Inc.</i> , 80 F.3d 1372 (9th Cir. 1996).....	22
<i>Weston v. Lockheed Missiles & Space Co.</i> , 881 F.2d 814 (9th Cir. 1989).....	26
<i>Warth v. Seldin</i> , 422 U.S. 490 (1975)	23
<i>Zuckerbraun v. General Dynamics Corp.</i> , 935 F.2d 544 (2d Cir. 1991).....	27, 51

Statutes

18 U.S.C. § 2510(11)	25
18 U.S.C. § 2511(1)(a).....	6
18 U.S.C. § 2511(1)(c).....	6
18 U.S.C. § 2511(1)(d).....	6
18 U.S.C. § 2511(3)(a).....	6
18 U.S.C. § 2702(a)(1).....	6
18 U.S.C. § 2702 (a)(2).....	6
18 U.S.C. § 2702(a)(3).....	6
18 U.S.C. § 2711(1)	25
28 U.S.C. § 1292(b)	3, 5
28 U.S.C. § 1331	3
47 U.S.C. § 605	6
50 U.S.C. § 1801 <i>et seq.</i>	25
50 U.S.C. § 1801(k)	25
50 U.S.C. § 1810	25
50 U.S.C. § 1809	6
Cal. Bus. & Prof. Code § 17200 <i>et seq.</i>	6

Other Authorities

Letter from Alberto R. Gonzales, Att’y Gen., to Patrick Leahy, Chairman, Comm. on the Judiciary, and Arlen Specter, Ranking Member, Comm. on the Judiciary (Jan. 17, 2007), *available at* <http://leahy.senate.gov/press/200701/1-17-07%20AG%20to%20PJL%20Re%20FISA%20Court.pdf> 9

Niall McKay, *Lawmakers Raise Questions About International Spy Network*, N.Y. Times, May 27, 1999, *available at* <http://www.nytimes.com/library/tech/99/05/cyber/articles/27network.html> 39

PRELIMINARY STATEMENT

Plaintiffs Tash Hepting, *et al.* (“Plaintiffs”) allege in this case that Defendant AT&T Corp. (“AT&T”) violated federal law by assisting the government in certain alleged surveillance programs. Plaintiffs do not have standing to press such claims unless they can show, at a minimum, with respect to each alleged program: (1) that AT&T in fact assisted in the alleged program and (2) that Plaintiffs’ own communications were in fact intercepted and accessed by the government under the alleged program.

The United States, however, has asserted the state secrets privilege as to whether, among other things, AT&T assisted in any alleged surveillance program, and as to which individuals’ communications, if any, were intercepted and analyzed under any such alleged programs. In a declaration under penalty of perjury submitted in this case, Director of National Intelligence John Negroponte, the nation’s highest ranking intelligence officer, stated that revealing such information could “cause exceptionally grave damage to the national security of the United States.” Negroponte Decl. ¶ 9 (Excerpts of Record (“ER”) 57-58).¹

In light of that invocation of the state secrets privilege, Plaintiffs will not have access to the evidence necessary to establish standing, and, just as important,

¹ Director Negroponte was succeeded by John McConnell on February 20, 2007.

AT&T will be prevented from tendering any evidence that would disprove it. Firmly established precedent mandates that a case must be dismissed whenever it becomes clear that the state secrets privilege will prevent a plaintiff from proving a necessary element of his case *or* a defendant from defending itself fully on an issue.² In cases such as this one, where there is “no hope of a complete record and adversarial development of the issue,” the only proper result is to dismiss the complaint.³

Indeed, it would be fundamentally “unfair” to AT&T to subject it to continued litigation where the state secrets privilege will preclude AT&T from rebutting any allegations that Plaintiffs make in support of standing.⁴ This case cannot and should not go forward where AT&T is disabled from responding to allegations or evidence tendered by the plaintiffs, and is therefore deprived of the ability to defend itself against potentially massive liability. Moreover, as this Court has explained, although a dismissal in contexts like this one may appear “harsh” for the individual plaintiffs, the “greater public good,” and “ultimately the

² See *Kasza v. Browner*, 133 F.3d 1159, 1166 (9th Cir. 1998).

³ *Halkin v. Helms*, 690 F.2d 977, 1000 (D.C. Cir. 1982) (“*Halkin IP*”). See also *El-Masri v. United States*, No. 06-1667, 2007 WL 625130, at *8-*9 (4th Cir. Mar. 2, 2007).

⁴ See *Halkin v. Helms*, 598 F.2d 1, 11 (D.C. Cir. 1978) (“*Halkin P*”).

less harsh remedy,” is the protection of military and intelligence secrets the release of which could harm the public’s safety.

The brief of the United States provides a full explanation of the district court’s errors in applying the state secrets privilege and the *Totten* doctrine.⁵ This brief explains why the state secrets doctrine precludes the parties from fully and fairly litigating standing. Because the state secrets privilege prevents full litigation of that issue, this Court should reverse the district court and remand the matter with instructions to dismiss for lack of jurisdiction.

JURISDICTION

The district court had jurisdiction pursuant to 28 U.S.C. § 1331 because Plaintiffs brought claims under federal law. This Court has jurisdiction pursuant to 28 U.S.C. § 1292(b), under which it granted petitions for permission to appeal on November 7, 2006. *See* ER 340.

ISSUE PRESENTED FOR REVIEW

Whether the state secrets privilege prevents full and fair litigation regarding Plaintiffs’ standing and therefore requires dismissal.

⁵ The *Totten* doctrine is a threshold rule of justiciability that prevents litigation of any matter that would require disclosure of an alleged secret espionage agreement with the government. *See Tenet v. Doe*, 544 U.S. 1 (2005).

STATEMENT OF THE CASE

On January 31, 2006, Plaintiffs brought suit on behalf of a putative nationwide class of subscribers to the telephone or Internet services of AT&T after September 2001. They filed a first amended complaint (the “Complaint”) on February 22, 2006, which added a subclass of California residents. Plaintiffs alleged that AT&T unlawfully gave the National Security Agency (“NSA”) access to the contents of its customers’ communications and transaction records in conjunction with counterterrorism intelligence activities of the NSA. Specifically, their allegations were based on three categories of purportedly unlawful activity: (1) cooperation in the “Terrorist Surveillance Program” (“TSP”), a program the existence (but not the methods or details) of which the government has acknowledged and that entails only the interception of international communications involving at least one party believed to be affiliated with al Qaeda; (2) cooperation in an allegedly broader program of *untargeted* content surveillance that the United States has not confirmed; and (3) the sharing of databases of *records* containing non-content call detail information as part of a claimed “data-mining” program that the government also has never acknowledged.⁶

⁶ Although the Complaint does not always clearly distinguish among the categories of surveillance activity on which it is based, for the sake of analytical clarity, we

AT&T moved to dismiss on April 28, 2006, arguing, among other things, that Plaintiffs could not establish standing. On May 13, 2006, the United States moved to intervene as a defendant. Director of National Intelligence John Negroponte formally asserted the military and state secrets privilege on behalf of the United States, and on that basis the United States moved to dismiss and sought summary judgment.

On July 20, 2006, the district court denied both motions to dismiss. *See Hepting v. AT&T Corp.*, 439 F. Supp. 2d 974 (N.D. Cal. 2006) (ER 308-39). The court *sua sponte* certified the order for interlocutory appeal under 28 U.S.C. § 1292(b), recognizing that “there is a substantial ground for difference of opinion” regarding its conclusions. *Id.* at 1011 (ER 339).

On July 31, 2006, AT&T and the United States petitioned this Court for permission to appeal.⁷ Plaintiffs cross-petitioned and responded. On November 7,

identify them separately. All of Plaintiffs’ claims are based on one or more of these categories of conduct.

⁷ On August 9, 2006, the *Hepting* court became the transferee court for Multi-District Litigation (“MDL”) No. 1791, *In re NSA Telecommunications Records Litigation*, which comprises several dozen actions against AT&T, other telecommunications carriers, and the United States. Two transferor courts have also addressed state secrets issues similar to those in this appeal. *See Terkel v. AT&T Corp.*, 441 F. Supp. 2d 899 (N.D. Ill. 2006); *Al-Haramain Islamic Found., Inc. v. Bush*, 451 F. Supp. 2d 1215 (D. Or. 2006).

2006, this Court granted AT&T's and the Government's petitions, and denied Plaintiffs' cross-petition "as unnecessary." ER 340.

STATEMENT OF FACTS

A. Plaintiffs' Allegations

Plaintiffs allege – almost entirely “[o]n information and belief” – that AT&T has given the NSA and unspecified “other government agencies” “direct access” to AT&T’s “key telecommunications facilities and databases” in conjunction with counterterrorism surveillance activities authorized by the President. Compl. ¶¶ 6, 42 (ER 3, 9).⁸ Plaintiffs do not allege that AT&T conducted any electronic surveillance for its own purposes. Rather, the gravamen of the Complaint is that AT&T provided access to its databases and telecommunications facilities, and thereby enabled the government to obtain and review its customers’ communications and transaction records. *See id.* ¶¶ 6, 38, 41-42, 46, 51, 61 (ER 3, 8-10, 12). On this basis, Plaintiffs make claims under the First and Fourth Amendments, five federal statutes,⁹ and California’s unfair competition law, Cal. Bus. & Prof. Code § 17200 *et seq.* *See id.* ¶¶ 78-149 (ER 17-29). They seek injunctive and declaratory relief and massive monetary damages based on AT&T’s

⁸ Nothing in this brief should be taken as an admission or denial, tacit or express, of any allegation that AT&T participated in any activity alleged in the Complaint.

⁹ 18 U.S.C. § 2511(1)(a), (1)(c), (1)(d), (3)(a); 18 U.S.C. § 2702(a)(1), (a)(2); 18 U.S.C. § 2702(a)(3); 47 U.S.C. § 605; 50 U.S.C. § 1809.

alleged assistance to the NSA in connection with one or more of three categories of counterterrorism surveillance activity. *See id.*, Prayer for Relief (ER 29-31).

1. The TSP

Plaintiffs generally allege a “classified surveillance program” that “intercept[s] the telephone and Internet communications of people inside the United States without judicial authorization.” Compl. ¶ 32 (ER 7). The government has admitted the existence of a targeted program of communications content surveillance – the now-defunct Terrorist Surveillance Program, or TSP. This is the *only* category of surveillance alleged in the Complaint that the government has officially acknowledged, even in general terms. Even as to this category, the government has not acknowledged the methods used to accomplish the electronic interception, whether those methods involve any assistance from private parties, and, if so, which parties. The government also has not identified any individuals whose communications were intercepted under this program.

The existence of the TSP was reported by the *New York Times* on December 16, 2005, in an article asserting that, in the wake of the September 11, 2001 attacks, President Bush authorized the NSA to monitor the international calls and e-mail messages of individuals located within the United States with possible links to al Qaeda. *See* James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. Times, Dec. 16, 2005, at A1 (ER 36). Following publication

of the *New York Times* article, the President confirmed the existence of the TSP, as did Attorney General Gonzales.¹⁰ The President and the Attorney General explained that the TSP intercepted “contents of communications where . . . one party to the communication is outside the United States” and where the government has “a reasonable basis to conclude that one party to the communication is a member of al Qaeda, affiliated with al Qaeda, or a member of an organization affiliated with al Qaeda, or working in support of al Qaeda.” Gonzales/Hayden Press Briefing (ER 46).

In their Complaint, Plaintiffs did not allege that they engaged in international communications with al Qaeda members or affiliates and specifically excluded from their putative class any foreign powers or agents of foreign powers, including “anyone who knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor[.]” Compl. ¶ 70 (ER 14). In their opposition to the motion to dismiss, moreover, Plaintiffs argued that their Complaint was not founded on the TSP but rather addressed only a “broader Program” of “*untargeted*” surveillance. Pls.’ Opp’n to Mot. To Dismiss Am. Compl. at 2 (filed June 6, 2006) (Dkt. 176).

¹⁰ See President’s Radio Address (Dec. 17, 2005) (ER 43-44); Press Briefing by Attorney General Alberto Gonzales and General Michael Hayden, Principal Deputy Director for National Intelligence (Dec. 19, 2005) (“Gonzales/Hayden Press Briefing”) (ER 46-53).

On January 17, 2007, the Attorney General announced that the Foreign Intelligence Surveillance Court (“FISC”) has authorized the government “to target for collection international communications into or out of the United States where there is probable cause to believe that one of the communicants is a member or agent of al Qaeda or an associated terrorist organization.” Accordingly, “any electronic surveillance that was occurring as part of the [TSP] will now be conducted subject to the approval of the [FISC].” Letter from Alberto R. Gonzales, Att’y Gen., to Patrick Leahy, Chairman, Comm. on the Judiciary, and Arlen Specter, Ranking Member, Comm. on the Judiciary (Jan. 17, 2007), *available at* <http://leahy.senate.gov/press/200701/1-17-07%20AG%20to%20PJL%20Re%20FISA%20Court.pdf>.

2. Untargeted Content Surveillance

Plaintiffs also allege a broader program of untargeted “dragnet” surveillance of communications content. Plaintiffs allege, “[o]n information and belief,” that “AT&T Corp. has provided and continues to provide the government with direct access to all or a substantial number of the communications transmitted through its key domestic telecommunications facilities.” Compl. ¶ 42 (ER 9). According to Plaintiffs, this has allowed “NSA personnel [to] intercept[] large volumes of domestic and international telephone and Internet traffic in search of patterns of interest.” *Id.* ¶ 38 (ER 8). As the district court stated, any such untargeted content

surveillance was allegedly “of far greater scope than the publicly disclosed ‘terrorist surveillance program.’” 439 F. Supp. 2d at 994 (ER 325).

Plaintiffs indicated in the district court that their allegations regarding this alleged program are based on two declarations submitted in support of a motion for preliminary injunction. The first is from a former AT&T technician, Mark Klein (ER 66-73); the second is from J. Scott Marcus, a putative expert who reviewed the Klein declaration as well as proprietary documents Klein took from AT&T (ER 74-113). In response to those declarations, the government’s counsel represented to the district court that “Mr. Klein and Marcus never had access to any of the relevant classified information here, and with all respect to them, through no fault or failure of their own, they don’t know anything.” Tr. of Proceedings at 76 (June 23, 2006) (“6/23/06 Tr.”) (ER 189) (Ass’t Att’y Gen. Keisler).

The United States has never confirmed the existence of any untargeted content surveillance program of the kind alleged by Plaintiffs, much less that AT&T was involved in any such program or that Plaintiffs’ communications were intercepted under such a program. As the district court stated, “[t]he existence of this alleged program and AT&T’s involvement, if any, remain far from clear.” 439 F. Supp. 2d at 994-95 (ER 325).

3. Communications Records

Finally, Plaintiffs allege that, in addition to communications *content*, the government unlawfully accessed communications *records*. *See* Compl. ¶¶ 2, 6, 51-53 (ER 2-3, 10-11). Plaintiffs allege that AT&T gave the government “direct access to [AT&T’s] databases of stored telephone and Internet records,” including “records concerning communications to which Plaintiffs and class members were a party.” *Id.* ¶¶ 51-52 (ER 10). These records are alleged to include the originating and terminating telephone numbers and the time and length of “nearly every telephone communication carried over [AT&T’s] domestic network since approximately 2001,” as well as “records pertaining to Plaintiffs’ and class members’ use of AT&T Corp. long distance service and dial-up Internet service, including but not limited to [dialing, routing, addressing and/or signaling] information and personally identifiable customer proprietary network information.” *Id.* ¶¶ 55-56 (ER 11); *see also id.* ¶ 60 (ER 12).

As with the alleged program of untargeted content surveillance, the United States has never confirmed the existence of the alleged records program or commented on AT&T’s supposed involvement or the scope of any records collection. Here, too, the district court found that “the general contours and even the existence of the alleged communication records program remain unclear,” and

that “AT&T has neither confirmed nor denied its involvement” in such a program. 439 F. Supp. 2d at 997 (ER 328).

B. The United States’ and AT&T’s Motions To Dismiss

The United States moved to dismiss the Complaint or, in the alternative, for summary judgment, on the basis of the state secrets privilege. *See* Mem. in Supp. of U.S. Mot. To Dismiss at 14-16 (filed May 13, 2006) (Dkt. 124); *see also* U.S. Reply in Supp. of Mot. To Dismiss at 3-5 (filed June 16, 2006) (Dkt. 245).

In support of its state secrets assertions, the government filed public and classified declarations from Director of National Intelligence Negroponte (ER 54-60), and the Director of the NSA, General Keith B. Alexander (ER 61-65). In his public declaration, Director Negroponte explained that “any attempt to proceed in the case will substantially risk the disclosure of the privileged information” in question “and will cause exceptionally grave damage to the national security of the United States.” Negroponte Decl. ¶ 9 (ER 57-58). In particular, the Director of National Intelligence asserted that “[t]he United States can neither confirm nor deny allegations concerning intelligence activities, *sources*, methods, relationships, *or targets*,” specifically including “*allegations about NSA’s purported involvement with AT&T.*” *Id.* ¶ 12 (ER 58) (emphases added). He further explained that the United States could not confirm or deny that any particular person’s communications had been intercepted, because “disclosure of those who are

targeted by such activities would compromise the collection of intelligence information.” *Id.*

The United States argued that dismissal was required in light of this sworn declaration from the government’s most senior intelligence official. It explained that, under this Court’s decision in *Kasza*, where, as here, the state secrets privilege has been properly invoked and there is a reasonable danger that national security would be harmed, the privilege is ““absolute,”” and does not permit any “balanc[ing]” of the private interests of plaintiffs. Mem. in Supp. of U.S. Mot. To Dismiss at 10 (Dkt. 124) (quoting 133 F.3d at 1166). In this instance, the privilege mandated dismissal because it prevented litigation of all the claims in the Complaint: “Adjudicating each claim in the Amended Complaint would require confirmation or denial of the existence, scope, and potential targets of alleged intelligence activities, as well as AT&T’s alleged involvement in such activities,” none of which could be revealed without “causing exceptionally grave damage to the national security.” *Id.* at 16. At “every step in this case,” Plaintiffs’ ability “to prove their claims” *and* Defendants’ ability “to defend them” would require access to “privileged information.” *Id.*

Turning specifically to the issue of standing, the government cited the dismissal of similar cases involving alleging electronic surveillance where the state secrets privilege prevented adjudication of whether particular plaintiffs’

communications had been intercepted by the government and thus precluded a judicial determination of standing. *See id.* at 16-20 (citing *Halkin I*, *Halkin II*, and *Ellsberg v. Mitchell*, 709 F.2d 51 (D.C. Cir. 1983)). The government argued that, for closely analogous reasons, standing could not be properly litigated here. In particular, without confirmation “whether AT&T was involved with any such activity” or “whether a particular individual’s communications were intercepted,” “Plaintiffs ultimately will not be able to prove injury-in-fact or causation.” *Id.* at 18.

AT&T also moved to dismiss for lack of standing on similar grounds. *See* AT&T Mem. in Supp. of Mot. To Dismiss Am. Compl. at 19-25 (filed Apr. 28, 2006) (Dkt. 86); *see also* AT&T Reply Mem. in Supp. of Mot. To Dismiss Am. Compl. at 14-18 (filed June 16, 2006) (Dkt. 244). As AT&T explained, plaintiffs cannot establish any of the facts necessary for them to have standing “without information covered by the state secrets privilege,” and AT&T is equally disabled from disputing allegations related to standing. *Id.* at 17.

C. The District Court’s Decision

The district court denied the motions to dismiss. The district court first disagreed with Director Negroponte’s determination that whether AT&T provided assistance to the NSA in connection with the TSP is a state secret. In determining what constitutes a state secret, the district court said it would “look only at publicly

reported information that possesses substantial indicia of reliability,” 439 F. Supp. 2d at 990 (ER 322), and would exclude “mere assertions of knowledge by an interested party,” such as the Klein and Marcus declarations, *id.*

Purporting to consider “only public admissions or denials by the government, AT&T and other telecommunications companies,” *id.*, the district court held that “AT&T and the government have for all practical purposes already disclosed that AT&T assists the government in monitoring communication content,” *id.* at 991-92 (ER 323). The district court reached this conclusion by reasoning: (1) the United States has admitted the existence of the TSP, *see id.* at 992 (ER 323); (2) “it is inconceivable that this program could exist without the acquiescence and cooperation of some telecommunications provider,” *id.*; (3) AT&T is one of the largest telecommunications providers in the country, so its assistance “would greatly help” the government, and “whether this program could even exist without AT&T’s . . . cooperation” is “unclear,” *id.*; (4) that “AT&T’s history of cooperating with the government on such matters is well known,” because AT&T has reported that it has classified contracts with the government and has employees with security clearances, *id.*; and (5) that AT&T has admitted that it helps the government within lawful bounds and that it believes assistance in the alleged programs would have been legal, *see id.* at 992-93 (ER 324). The court thus concluded that “AT&T’s assistance in national security surveillance is hardly

the kind of ‘secret’ that the *Totten* bar and the state secrets privilege were intended to protect or that a potential terrorist would fail to anticipate.” *Id.* at 993 (ER 324). This conclusion directly contradicts the judgment of the Director of National Intelligence. *Compare id. with* Negroponte Decl. ¶¶ 9, 12 (ER 57-59).

The district court never specifically found that Plaintiffs could establish that they were targeted by the TSP or that they had standing to challenge that program. But, from its conclusion that AT&T must be participating in the TSP, and therefore that AT&T’s presumed participation was not a state secret, the court extrapolated to find that standing could be established to challenge the *different* alleged untargeted content surveillance program. The court construed the Complaint to allege an all-encompassing surveillance “dragnet” in which the government obtained the contents of the communications of AT&T’s subscribers (including Plaintiffs’) and found this sufficient to allege injury-in-fact, causation, and redressability. *See* 439 F. Supp. 2d at 1000-01 (ER 331).

In response to the argument that, regardless of their allegations, Plaintiffs would not be able to *establish* their standing – and that AT&T would be disabled from rebutting any claims that Plaintiffs make – without access to state secrets, the district court held that the state secrets privilege would not prevent Plaintiffs from receiving “at least some evidence tending to establish the factual predicate for the injury-in-fact” underlying these claims. *Id.* at 1001 (ER 331). The court

contradicted its decision to exclude “mere assertions of knowledge” by interested parties like Klein and Marcus by indicating that their declarations furnish “at least some factual basis for plaintiffs’ standing.” *Id.* at 990, 1001 (ER 322, 332).

Moreover, the court stated that the state secrets privilege would not prevent Plaintiffs from receiving discovery relating to whether the government had provided AT&T with a “certification” under 18 U.S.C. § 2511(2)(a)(ii), which would bar all claims against AT&T. *See id.* at 996-97, 1001 (ER 328, 332). The district court recognized “that uncovering whether and to what extent a certification exists might reveal information about AT&T’s assistance to the government that has not been publicly disclosed.” *Id.* at 995 (ER 326).

Nonetheless, the court reasoned that because the President had denied in general terms the existence of indiscriminate surveillance, he “opened the door for judicial inquiry.” *Id.* at 996 (ER 328). On that basis, the court held that AT&T could be required to confirm or deny the existence of a certification “through a combination of responses to interrogatories and *in camera* review by the court” at a level of generality that assertedly would not compromise any information not already made public. *Id.* at 996-97 (ER 328). The court did not explain how discovery on the certification issue could demonstrate whether Plaintiffs’ particular communications had been ensnared in the alleged “dragnet.”

With respect to the call records program, the district court recognized that, like the alleged untargeted content surveillance program, the existence of a records program was “unclear.” *See id.* at 997 (ER 328). Here, however, the court concluded that any discovery into the asserted records program would violate the state secrets privilege. *See id.* Nonetheless, the court refused to dismiss claims based on the records allegations, because “additional facts might very well be revealed during, but not as a direct consequence of, this litigation that obviate many of the secrecy concerns currently at issue regarding the alleged communication records program.” *Id.* at 1001 (ER 331-32).

SUMMARY OF ARGUMENT

As this Court explained in *Kasza*, when the state secrets doctrine prevents full and fair litigation of any necessary issue (including standing), or deprives the defendant of the ability to defend itself fully on such an issue, the proper course is to dismiss the case as soon as this is apparent. In this case, as in *Halkin I*, *Halkin II*, and other prior cases involving alleged government surveillance, it is clear right now that the state secrets privilege will prevent adjudication of standing.

Accordingly, the district court should have dismissed the Complaint forthwith, without permitting further litigation that unnecessarily risks disclosure of sensitive national security information but will never result in full adjudication of this

threshold jurisdictional issue. The court should have found that standing cannot be litigated for two independent reasons.

First, Plaintiffs cannot prove, and AT&T cannot refute, the assertion that AT&T caused them injury because, as Director of National Intelligence Negroponte emphasized in his declaration, the identity of any source of intelligence for the programs alleged here – whether AT&T or any other carrier – is a state secret, the disclosure of which threatens grave harm to national security.

Instead of granting the “utmost deference” to that conclusion of the government’s highest ranking intelligence official, as required by *Kasza*, 133 F.3d at 1166, the district court used a chain of conjecture, hypothesis, and unwarranted inference to suggest that AT&T’s alleged participation in these programs was not in fact a secret. The court, for instance, relied on its own unfounded and inexpert speculation that content surveillance requires the cooperation of a telecommunications provider. The court similarly speculated that AT&T, because of its size, must have been involved in any such program. The district court’s decision to rely on these and other hypotheses to overcome the assertion of the state secrets privilege by the Director of National Intelligence is misguided and improper.

Second, Plaintiffs cannot prove, and AT&T cannot refute, whether any of these purported programs injured them because no Plaintiff can show that *his or*

her own communications or records were intercepted under these alleged programs.

Plaintiffs apparently no longer claim injury from the targeted TSP. Even if that were not the case, Director Negroponte has identified the targets of that program as a state secret, and the district court provided no basis to override that judgment.

As to Plaintiffs' claims of harm from *untargeted* content surveillance, the government has not acknowledged the existence of any such program, and any information about the methods or targets of alleged government surveillance is unquestionably covered by Director Negroponte's invocation of the state secrets doctrine. The district court tried to circumvent that privilege assertion by reading Plaintiffs' Complaint to allege that *all* AT&T customers were subject to surveillance, so that Plaintiffs were necessarily injured. But the Complaint carefully avoids any such allegation. More importantly, even if Plaintiffs could make such an allegation, proving that allegation would require discovery of the very operational details, of what is allegedly an ongoing but unacknowledged program of counterterrorism surveillance, that are at the heart of the state secrets privilege. Plaintiffs could not prove, and AT&T could not contest, that their own communications were captured in any such program without access to state secrets. In such cases, where there is "no hope of a complete record and adversarial

development of the issue,” the only proper result is to dismiss the Complaint.

Halkin II, 690 F.2d at 999-1000.

The declarations of Klein, a former AT&T technician, and Marcus, a putative expert who reviewed materials provided by Klein, do not provide any basis to litigate this issue. As statements of private parties, they cannot waive the state secrets privilege. Nor are those individuals “indisputably situated to disclose” reliable information, as the district court elsewhere acknowledged would be necessary. 439 F. Supp. 2d at 990 (ER 322). At least as significant, because of the government’s assertion of the state secrets privilege, their declarations cannot be tested and countered by AT&T. In all events, even on their own terms, these declarations do not claim that the government engaged in blanket surveillance of all AT&T customers.

Nor can the discovery that the district court has (improperly) stated that it will consider serve to circumvent the barrier posed by the state secrets privilege to full and fair litigation of standing. The discovery considered by the court relates only to whether AT&T received a statutory authorization to participate in alleged warrantless surveillance. Even the district court did not permit the extraordinary revelation of secret program details, if any exist, that would be necessary to allow the Court to decide on a full record whether these particular Plaintiffs were injured

under this alleged program. Because such discovery on this core jurisdiction issue is plainly impossible here, the court should have dismissed the case.

Finally, the district court properly held that whether there is a communications records program is a state secret, and it precluded discovery regarding any such alleged program. The court erred, however, in declining to dismiss even these parts of the Complaint, because, it speculated, future leaks might reveal further information. If Plaintiffs cannot prove standing now, the district court lacks jurisdiction, and dismissal now is the only proper course.

STANDARD OF REVIEW

This Court reviews jurisdictional determinations and denials of motions to dismiss for failure to state a claim *de novo*. See, e.g., *Vinci v. Waste Mgmt., Inc.*, 80 F.3d 1372, 1374 (9th Cir. 1996); *King County v. Rasmussen*, 299 F.3d 1077, 1088 (9th Cir. 2002).

ARGUMENT

I. LITIGATION MUST BE DISMISSED WHEN THE STATE SECRETS DOCTRINE PRECLUDES THE PARTIES FROM FULLY AND FAIRLY LITIGATING THE THRESHOLD ISSUE OF STANDING

A. Plaintiffs Must Prove That They Were Subjected to the Alleged Surveillance and That AT&T Assisted in That Activity

A threshold question in every federal case is whether the party bringing the suit can establish its standing. In order to have standing, the plaintiff must demonstrate (1) “an ‘injury in fact’”; (2) “a causal connection between the injury

and the conduct of which the party complains”; and (3) “that it is ‘likely’ a favorable decision will provide redress.” *Kowalski v. Tesmer*, 543 U.S. 125, 129 n.2 (2004). A plaintiff must prove that he “‘*personally* has suffered some actual or threatened injury as a result of the putatively illegal conduct of the defendant.’” *Valley Forge Christian Coll. v. Americans United for Separation of Church & State, Inc.*, 454 U.S. 464, 472 (1982) (emphasis added). Regardless of whether “‘an injury [is] shared by a large class of other possible litigants,’” “a plaintiff ‘must allege a distinct and palpable injury to himself.’” *Pony v. County of Los Angeles*, 433 F.3d 1138, 1145 (9th Cir.) (quoting *Warth v. Seldin*, 422 U.S. 490, 501 (1975)), *cert. denied*, 126 S. Ct. 2864 (2006). This is equally true in class actions: unless a named plaintiff can establish that he personally suffered actual injury, he cannot sue on behalf of himself or a class, no matter who else may have been injured. *See Warth*, 422 U.S. at 502; *Casey v. Lewis*, 4 F.3d 1516, 1519 (9th Cir. 1993). Moreover, a plaintiff must establish that his injury-in-fact was caused by the defendant, and not “some third party not before the court.” *Simon v. Eastern Ky. Welfare Rights Org.*, 426 U.S. 26, 41-42 (1976).

It is not sufficient merely to allege standing; the burden is upon the plaintiff to *demonstrate* each element of standing. *See Smelt v. County of Orange*, 447 F.3d 673, 682 (9th Cir.), *cert. denied*, 127 S. Ct. 396 (2006); *see also Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561 (1992). Thus, when challenged, a

plaintiff must come forward with facts demonstrating that he in fact suffered injury caused by the defendants. Where the facts are in dispute, a district court must resolve that dispute and determine its own jurisdiction. *See, e.g., id.* at 561; *Martin v. Morgan Drive Away, Inc.*, 665 F.2d 598, 602 (5th Cir. 1982).

A defendant must have a fair opportunity to contest standing and to challenge whatever facts the plaintiff may put forward in seeking to establish it. A defendant must be able to “attack the substance of a complaint’s jurisdictional allegations despite their formal sufficiency.” *Dreier v. United States*, 106 F.3d 844, 847 (9th Cir. 1997) (quoting *St. Clair v. City of Chico*, 880 F.2d 199, 201 (9th Cir. 1989)).

As applied to the surveillance context, these principles require that a plaintiff show – and that defendants be given a full opportunity to contest – that the plaintiff’s own communications or records were actually accessed by the government. When a plaintiff claims injury arising out of government surveillance, Article III standing exists only when the plaintiff can furnish “proof of actual acquisition of [his] communications.” *Halkin II*, 690 F.2d at 999-1000. Nothing short of that constitutes actual, concrete injury to a particular plaintiff from government surveillance. In a long line of cases, the federal courts have strictly adhered to this requirement. *See, e.g., Laird v. Tatum*, 408 U.S. 1, 18-20

(1972); *Halkin I*, 598 F.2d 1; *Ellsberg*, 709 F.2d at 65; *United Presbyterian Church v. Reagan*, 738 F.2d 1375, 1378 (D.C. Cir. 1984).¹¹

It is equally the case that, to meet the causation and redressability requirements of standing, the plaintiff must prove – and, again, the defendant must have a full opportunity to contest – that the *particular defendant* sued in the case was responsible for the interception. *See Tooley v. Bush*, No. 06-306, 2006 U.S. Dist. LEXIS 92274, at *80 (D.D.C. Dec. 21, 2006) (“relief would, of course, be entirely ineffective if, in fact, [a] Plaintiff is the subject of [surveillance] by someone other than [the defendant]”).

¹¹ The standing requirements in the federal statutes invoked by Plaintiffs require the same injury. For example, the Foreign Intelligence Surveillance Act (“FISA”), 50 U.S.C. §§ 1801 *et seq.*, affords a cause of action only to “[a]n aggrieved person . . . who has been subjected to an electronic surveillance.” *Id.* § 1810. An “[a]ggrieved person” is defined as “a person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance.” *Id.* § 1801(k). Accordingly, under FISA, a party “has no standing to assert the illegality of surveillances of communications to which he was not a party.” *United States v. Ott*, 637 F. Supp. 62, 64 (E.D. Cal. 1986), *aff’d*, 827 F.2d 473, 475 n.1 (9th Cir. 1987) (litigant had “standing to bring a motion” under FISA “[b]ecause [his] communications were subject to surveillance”); *see also United States v. Faulkner*, 439 F.3d 1221, 1223 (10th Cir. 2006) (“Generally, to establish standing [under the Wiretap Act] movant must show that (1) he was a party to the communication, (2) the wiretap efforts were directed at him, or (3) the interception took place on his premises.”); Stored Communications Act (“SCA”), 18 U.S.C. §§ 2711(1), 2510(11) (authorizing a civil action for “a person who was a party to any intercepted wire, oral, or electronic communication or a person against whom the interception was directed”) (emphases added).

B. When the State Secrets Privilege Prevents the Full and Fair Litigation of Standing, Dismissal Is Required

Standing, like every other aspect of a case, is subject to the invocation by the United States of the military and state secrets privilege. *See generally United States v. Reynolds*, 345 U.S. 1 (1952); *Halkin I*, 598 F.2d at 7. The state secrets privilege authorizes the federal government to “protect[] information from discovery when disclosure would be inimical to the national security.” *In re United States*, 872 F.2d 472, 474 (D.C. Cir. 1989). When “the government shows that ‘the information poses a reasonable danger to secrets of state,’” *id.* at 475, the privilege is “*absolute*” and not subject to any balancing of countervailing interests, *Ellsberg*, 709 F.2d at 57 (emphasis added).

In some cases, the only effect of the state secrets privilege is to suppress particular evidence. *See id.* at 64. This Court has recognized, however, that in many other cases the doctrine entirely precludes further litigation. *Kasza* establishes that dismissal is required if the state secrets privilege prevents the plaintiff from “prov[ing] the *prima facie* elements of her claim”; if it prevents the defendant from making out a defense; or “if the ‘very subject matter of the action’ is a state secret.” 133 F.3d at 1166.¹² Although dismissal in these circumstances

¹² Other courts have dismissed actions at the threshold when state secrets have removed a necessary element of proof from the case, *e.g.*, *Weston v. Lockheed Missiles & Space Co.*, 881 F.2d 814 (9th Cir. 1989); dismissed at later stages of

may be “harsh” for the individual plaintiffs, the “greater public good,” and “ultimately the less harsh remedy,” is the preservation of secrets important to the protection of the entire nation. 133 F.3d at 1167 (internal quotation marks omitted); *see also id.* at 1170 (affirming dismissal of Resource Conservation and Recovery Act case where state secrets privilege prevented release of data regarding hazardous wastes at particular facility; “any further proceeding in this matter would jeopardize national security”).

Similarly, in *El-Masri*, the Fourth Circuit recently concluded that “dismissal at the pleading stage is appropriate” if the state secrets privilege either prevents the plaintiff from establishing a *prima facie* case or “the defendants could not properly defend themselves without using privileged evidence.” 2007 WL 625130, at *8-*9; *see also McDonnell Douglas Corp. v. United States*, 323 F.3d 1006, 1021 (Fed. Cir. 2003); *Bareford*, 973 F.2d at 1144.

proceedings due to the unavailability of proof, *e.g.*, *Fitzgerald v. Penthouse Int’l, Ltd.*, 776 F.2d 1236 (4th Cir. 1985); granted summary judgment where state secrets prevented the plaintiff from establishing an element of its *prima facie* case, *e.g.*, *Bareford v. General Dynamics Corp.*, 973 F.2d 1138 (5th Cir. 1992); *Zuckerbraun v. General Dynamics Corp.*, 935 F.2d 544 (2d Cir. 1991); granted summary judgment or dismissed where the state secrets privilege prevented the defendant from making out a defense, *e.g.*, *Molerio v. FBI*, 749 F.2d 815, 820-22 (D.C. Cir. 1984); *Sterling v. Tenet*, 416 F.3d 338, 347 (4th Cir. 2005), *cert. denied*, 126 S. Ct. 1052 (2006); and dismissed where the very subject matter of the suit involved state secrets, notwithstanding production of non-privileged evidence sufficient to support a *prima facie* case, *e.g.*, *Farnsworth Cannon, Inc. v. Grimes*, 635 F.2d 268, 276 (4th Cir. 1980); *Fitzgerald*, 776 F.2d at 1243-44.

In sum, when it is apparent that the state secrets doctrine will prevent a court from fully and fairly adjudicating some element of a case that is essential to eventually reaching judgment, the case must be dismissed without further proceedings. *See, e.g., Halkin II*, 690 F.2d at 1000 (“With no hope of a complete record and adversarial development of the issue, we cannot authorize . . . [an] inquiry [into state secrets].”); *see also, e.g., id.* at 998-1000; *Kasza*, 133 F.3d at 1166; *Halkin I*, 598 F.2d at 11. As Judge Phillips recognized in a dissenting opinion that ultimately was vindicated by the Fourth Circuit sitting en banc, where “litigation [is] constrained by administration of the [state secrets] privilege” in such a way that it “simply could not afford the essential fairness of opportunity to both parties that is a fundamental assumption of the adversary system,” the case must be dismissed. *Farnsworth Cannon*, 635 F.2d at 279 (Phillips, J., dissenting); *see id.* at 281 (en banc) (per curiam); *cf. Philip Morris USA v. Williams*, 127 S. Ct. 1057, 1063 (2007) (“[T]he Due Process Clause prohibits a State from punishing an individual without first providing that individual with ‘an opportunity to present every available defense.’”) (quoting *Lindsey v. Normet*, 405 U.S. 56, 66 (1972)).

Moreover, given the risks posed by ongoing litigation in areas touching upon state secrets, the courts have an obligation to dismiss *as soon as* it becomes apparent that fair adjudication of any necessary element will be impossible. *See, e.g., El-Masri*, 2007 WL 625180, at *7-*8 (collecting cases requiring “dismissal at

the pleading stage” based on unavailability of privileged information that would be necessary to litigate fairly at later stages); *Farnsworth Cannon*, 635 F.2d at 281 (because in further litigation “the plaintiff and its lawyers would have every incentive to probe as close to the core [state] secrets as the trial judge would permit,” “the overriding interest of the United States and the preservation of its state secrets precludes any further attempt to pursue this litigation,” even if some further proceedings could take place solely with non-privileged evidence).

The principle that a case must be dismissed when the state secrets doctrine prevents a plaintiff from establish standing – and/or prevents a defendant from fully litigating that issue – has been applied repeatedly by the D.C. Circuit to dismiss cases involving alleged government surveillance.

In *Ellsberg*, a case that, like this one, involved alleged warrantless electronic surveillance, the government admitted (unlike in this case) that it had overheard communications of some of the plaintiffs. The court held that only those plaintiffs whom the government had admitted surveilling had standing; the lack of a similar admission “incapacitated” the other plaintiffs’ claims: “Membership in a group of people, one or more members of which were exposed to surveillance, is insufficient to satisfy [the injury-in-fact] requirement.” 709 F.2d at 65 (internal quotation marks omitted).

The *Halkin* cases similarly establish that where the state secrets privilege prevents litigation of standing, the case must be dismissed. In *Halkin I*, Vietnam War protesters sued various intelligence agencies and telecommunications carriers, challenging two NSA signals intelligence programs that involved the warrantless interception of international telecommunications and telegrams. The district court held that the state secrets privilege prohibited plaintiffs from demonstrating standing to challenge one of the programs, “*because the ultimate issue, the fact of acquisition, could neither be admitted nor denied.*” 598 F.2d at 5 (emphasis added). The court of appeals affirmed, and further held that the state secrets privilege foreclosed “confirmation or denial that a particular plaintiff’s communications have been acquired” in connection with the second program. *Id.* at 10.

In *Halkin II*, the court held that, notwithstanding the fact that “considerable detail” about the alleged surveillance programs had been made public, the case was required to be dismissed because plaintiffs merely had “alleged . . . concrete injury” but “*ultimately cannot show*” it. 690 F.2d at 999. The court explained that, “[a]s a result of [*Halkin I*], plaintiffs’ claims against the NSA and several individual officials connected with that agency’s monitoring activities could not be proved, and the complaint as to those defendants was dismissed.” *Id.* at 984. The court went on to consider whether the plaintiffs could bring a claim against the

CIA for submitting “watchlists” to the NSA. *Id.* at 984, 997. The court of appeals held that the plaintiffs could not demonstrate standing in this context either, because “*the absence of proof of actual acquisition of [plaintiffs’] communications is fatal* to their watchlisting claims.” *Id.* at 999-1000 (emphasis added).

II. PLAINTIFFS CANNOT ESTABLISH STANDING BECAUSE THE STATE SECRETS PRIVILEGE PRECLUDES ADJUDICATION OF WHETHER AT&T PARTICIPATED IN THE ALLEGED SURVEILLANCE ACTIVITIES

A. To Establish Standing, Plaintiffs Must Show That AT&T Participated in the Alleged Surveillance Activities, a Fact That Is Central to the Director of National Intelligence’s State Secrets Assertion

To establish standing, Plaintiffs must demonstrate that AT&T participated in the surveillance activities alleged in the Complaint. If Plaintiffs, who sue as AT&T subscribers, *see generally* Compl. ¶¶ 6, 13-16 (ER 3-4), cannot establish that AT&T assisted in those activities, they cannot establish *any* of the three basic standing requirements: that they suffered a concrete injury in the form of unlawful government acquisition of their communications, that AT&T caused that injury, or that the injury would be redressable through a judgment against AT&T.

The question whether AT&T participated in the alleged surveillance activities, however, falls squarely within the scope of the United States’ assertion of the state secrets privilege. In invoking the privilege, Director of National Intelligence Negroponte specifically identified “NSA’s purported involvement

with AT&T” as subject to the privilege and specified that release of information on that point, among others, would “cause exceptionally grave damage to the national security of the United States.” Negroponte Decl. ¶¶ 9, 12 (ER 57-58). Case law confirms that intelligence sources and methods, such as which private company’s facilities, if any, the NSA employs in conducting foreign intelligence surveillance, are among the categories of information that the state secrets privilege protects. *See Tenet v. Doe*, 544 U.S. at 11 (state secrets protects the identity of sources); *Sterling*, 416 F.3d at 346 (state secrets protects “intelligence-gathering methods or capabilities”) (internal quotation marks omitted); *Fitzgibbon v. CIA*, 911 F.2d 755, 762 (D.C. Cir. 1990) (sources and methods “constitute the heart of all intelligence operations”) (internal quotation marks omitted); *ACLU v. Brown*, 619 F.2d 1170, 1174 (7th Cir. 1980) (state secrets include “the means by which [surveillance] was accomplished”). As Assistant Attorney General Keisler represented to the district court, whether or not AT&T is “cooperating with the government in intelligence-gathering . . . is absolutely a secret; it’s a secret of the highest order.” 6/23/06 Tr. at 49-50 (ER 162-63).

There has never been any dispute in this case that the United States validly invoked the privilege as a procedural matter, and the district court so found. *See* 439 F. Supp. 2d at 993 (ER 324). Accordingly, unless that invocation can be ignored or overridden, the state secrets privilege precludes the district court from

finding the threshold fact on which any showing of standing would necessarily depend.

Moreover, for the reasons discussed above, *see supra* p. 26-28, even if Plaintiffs were able to *allege* AT&T's participation or to adduce facts that, if uncontested, might support an inference of participation, that would not be enough to allow this case to go forward. Rather, the district court, and this Court, would also need to be satisfied that AT&T could contest those allegations and have a fair opportunity to defend itself. *See, e.g., Halkin I*, 598 F.2d at 11 (affirming dismissal grounds where state secrets privilege would prevent defendants from "rebut[ting]" any presumption that plaintiffs' communications were acquired and thus would be "unfair"). Here, even assuming there were intelligence programs of the kind Plaintiffs have alleged, and even assuming evidence could be developed suggesting AT&T participated in them, the assertion of the privilege by the United States would prevent AT&T from contesting the allegations by introducing evidence relating to the nature or extent of its involvement. The parties could not litigate whether Plaintiffs' injury, assuming there were one, was fairly traceable to AT&T's conduct, nor could the parties litigate whether the relief sought against AT&T would redress the alleged harms. Under these circumstances, the case must be dismissed. *See, e.g., Kasza*, 133 F.3d at 1166 (judgment should be given to defendants where the state secrets privilege "deprives the defendant of information

that would otherwise give the defendant a valid defense”) (internal quotation marks omitted); *El-Masri*, 2007 WL 625130, at *8, *9 (dismissal required where “the defendants could not properly defend themselves without using privileged evidence”); *Halkin II*, 690 F.2d at 1000 (dismissal on standing grounds appropriate where there is “no hope of a complete record and adversarial development of the issue”).

B. The District Court Erred in Hypothesizing That AT&T Must Have Participated in the Alleged Programs

Plaintiffs sought to avoid dismissal on this ground by arguing that AT&T’s involvement in the alleged NSA programs *already* is public and therefore is not a state secret. The district court agreed, at least in part, concluding that “AT&T and the government have for all practical purposes already disclosed that AT&T assists the government in monitoring communication content.” 439 F. Supp. 2d at 991-92 (ER 323). But neither the government nor AT&T has ever admitted or denied – whether directly or indirectly, much less for “all practical purposes” – that AT&T is involved in any activity alleged in the Complaint. On the contrary, the government, through the declaration of Director Negroonte, has expressly asserted that whether AT&T assists in any such program is a state secret. *See* Negroonte Decl. ¶¶ 9, 12 (ER 57-59).

Presented with that proper invocation of the state secrets doctrine, the district court’s duty under the law of this Circuit was to engage in the “narrow”

review necessary to determine whether there is a “reasonable danger” to national security. *Kasza*, 133 F.3d at 1166 (requiring “utmost deference”) (quoting *Reynolds*, 345 U.S. at 10); *cf. Halkin I*, 598 F.2d at 7 (court must “be especially careful not to order any dissemination of information asserted to be privileged state secrets”). Here, however, the district court chose to speculate about whether there might be any basis to conclude that AT&T’s alleged participation was *not* a state secret. That, by itself, was error. And the district court’s decision is particularly improper because it relies on an inferential chain consisting of five links, *see supra* p. 15, each of which is mistaken, irrelevant, or dependent upon impermissible speculation.

First, the district court observed that the United States has admitted the existence of the TSP. *See* 439 F. Supp. 2d at 992 (ER 323). The targeted TSP, however, is the *only* surveillance program the existence of which the government has confirmed. There has been no admission of any other program – not untargeted content interception, and not access to communications records – and the district court recognized as much. *See id.* at 994-95 (ER 325). Even under the district court’s reasoning, Plaintiffs’ claims based on alleged surveillance activities other than the TSP would have to be dismissed.

Beyond that, Plaintiffs’ submissions indicate that they do not claim injury from the TSP. Whereas the TSP intercepts “one-end foreign’ communications

where one party is associated with the al Qaeda terrorist organization,” Negroponte Decl. ¶ 11 (ER 58), Plaintiffs have expressly disclaimed any connection with al Qaeda, *see* Compl. ¶¶ 13-16 (ER 4), and have defined the putative class in like terms, *see id.* ¶ 70 (ER 14). Indeed, Plaintiffs have admitted that their allegations are not meant to encompass a claim that they were surveilled, or therefore injured, by the TSP:

The gravamen of the Complaint is not that plaintiffs have some unspecified fear that they *may* have been wrongfully ensnared in the Terrorist Surveillance Program, as AT&T claims. Instead, it alleges that plaintiffs[] *have already been* ensnared in the broader Program’s fishing expedition through the entirety of AT&T’s networks and databases.

See Pls.’ Opp’n to Mot. To Dismiss Am. Compl. at 2 (Dkt. 176). Thus, even under the district court’s own flawed reasoning, any supposed public acknowledgement of AT&T’s participation is irrelevant, as Plaintiffs themselves have indicated that the targeted TSP acknowledged by the government is not the basis for their claims.

Moreover, precedent establishes that the mere confirmation of the existence of a program does not eliminate state secrets protection for details, such as sources and methods, that have not been disclosed. Thus, the Fourth Circuit recently rejected plaintiff’s claim that, because a program of “extraordinary rendition” had been publicly acknowledged by the President and other government officials and “widely discussed in public forums,” the state secrets privilege would not bar litigation by an alleged target of that program. *El-Masri*, 2007 WL 625130, at *1,

*2. “The controlling inquiry,” the Court explained, “is not whether the general subject matter of an action can be described without resort to state secrets,” but rather whether the action “can be *litigated* without threatening disclosure of such state secrets.” *Id.* at *8 (emphasis in original). Because the specifics of the rendition program – including the “means and methods” employed by the CIA and whether “the defendants were involved in [the] detention” at issue – were not known to the public and were properly privileged, the case had to be dismissed. *Id.* at *16-*17.

Numerous other cases are to the same effect. *See, e.g., Totten v. United States*, 92 U.S. 105 (1875) (dismissing a suit alleging a secret espionage agreement between William Lloyd and the United States government where Lloyd’s estate itself asserted the relationship existed); *Halkin I*, 598 F.2d at 10 (even though the district court “thought congressional committees investigating intelligence matters had revealed so much information about [an NSA program] that . . . disclosure would pose no threat to the NSA mission,” the court of appeals reversed because the specific information over which the government claimed the privilege – whether plaintiffs’ own communications were acquired – remained undisclosed); *Halkin II*, 690 F.2d at 994 (“We reject . . . the theory that because *some* information about the project ostensibly is now in the public domain, *nothing* about the project in which the appellants have expressed an interest can properly remain

classified or otherwise privileged from disclosure.”) (internal quotation marks omitted); *Hayden v. NSA*, 608 F.2d 1381, 1388 (D.C. Cir. 1979) (rejecting the argument that “some channels monitored by NSA are well known to be closely watched, and that no foreign government would send sensitive material over them; hence NSA can safely disclose material” regarding those channels). Thus, the acknowledgement of the existence of the TSP does nothing to remove state secrets protection as to the details of that program, including most importantly whether AT&T participated in it.

Second, the court speculated that it was “inconceivable” that the TSP “could exist without the acquiescence and cooperation of some telecommunications provider.” 439 F. Supp. 2d at 992 (ER 323). The court offered no support for its speculation – which, again, applies *only* to the TSP – and for good reason: no operational details of the TSP have been disclosed. “This is precisely the sort of conjecture [the courts] may not entertain in assessing standing.” *DaimlerChrysler Corp. v. Cuno*, 126 S. Ct. 1854, 1866 (2006). And there is no reason to assume that the court’s conjecture is correct. There may be any number of ways in which the government might be able to carry out surveillance without the participation of telecommunications carriers – by intercepting satellite signals, covertly tapping or splicing into carrier cables (undersea or elsewhere), or by employing interception

technologies that are simply unknown to the public.¹³ For a district court to ground conclusions about standing and its own jurisdiction on pure speculation about what the court thinks is or is not “inconceivable” would be problematic under any circumstances. It is thoroughly misguided and inconsistent with the “utmost deference” mandated by *Kasza* to rely on such speculation to override the considered judgment of the Director of National Intelligence on an issue squarely within his expertise and that relates to the technical and covert realm of signals intelligence. *See Halkin I*, 598 F.2d at 10-11 (refusing to ground standing on assumptions about intelligence operations in state secrets case).

Third, the district court asserted that, because “some telecommunications provider” must have cooperated with the TSP, that provider must be AT&T because of its size. 439 F. Supp. 2d at 992 (ER 323). According to the court, “[c]onsidering the ubiquity of AT&T telecommunications services, it is unclear whether this program could even exist without AT&T’s acquiescence and cooperation.” *Id.* Again, this sort of unvarnished speculation does not establish standing. *See ASARCO v. Kadish*, 490 U.S. 605, 614 (1989) (Kennedy, J.). There is nothing in the record to support these opinions or inferences. Nor could there

¹³ *See generally* Niall McKay, *Lawmakers Raise Questions About International Spy Network*, N.Y. Times, May 27, 1999 (discussing alleged surveillance programs involving satellite signals and tapping into cables), available at <http://www.nytimes.com/library/tech/99/05/cyber/articles/27network.html>.

be, given that the operational details of even the TSP remain a state secret. Needless to say, there are other large telecommunications carriers in the United States. And AT&T's size and coverage say nothing about whether it has participated in any specific intelligence program, much less so incontrovertibly that an asserted state secret may be transformed into a presumed and established fact on which to ground standing to sue.

Notably, the court acknowledged that "it is unclear" whether the limited TSP could exist without AT&T's participation. 439 F. Supp. 2d at 992 (ER 323). That it is "unclear" whether AT&T participated even in the TSP means that this question remains a legitimate state secret. *A fortiori*, under no conceivable circumstances could AT&T's participation in some broader, unacknowledged program of untargeted content surveillance be so well-established as to justify overriding Director Negroponte's sworn statement that that matter is a state secret.

Fourth, the court reasoned that, because AT&T has participated in some unspecified classified work for the government in the past, it must have participated in the particular activities alleged here. *See id.* ("AT&T's history of cooperating with the government on such matters is well known."). Even assuming it were true that AT&T and the government have in the past had "some kind of intelligence relationship," *id.* at 994, 995 (ER 325, 326), such a supposition provides no support for the conclusion that AT&T participated *in the specific*

*programs alleged here.*¹⁴ This reasoning goes far beyond the inferences of propensity that the Federal Rules of Evidence would permit in a garden-variety case, *see generally* Fed. R. Evid. 404, 406, and is especially improper in a state secrets case.¹⁵ *See, e.g., Halkin I*, 598 F.2d at 10-11 (refusing to indulge as “manifestly unfair” a presumption of surveillance arising from appearance of target names on a CIA watchlist).

Fifth, and finally, the court purported to derive an admission of participation by cobbling together statements by an AT&T spokesman and a statement made at oral argument on the motion to dismiss. It noted AT&T’s statement that, “when AT&T is asked to help, we do so strictly within the law,” among similar statements. 439 F. Supp. 2d at 992 (ER 323) (internal quotation marks omitted). It then joined these statements with counsel’s assertion that “any such assistance [to the federal government] would be legal if AT&T were simply a passive agent of the government or if AT&T received a government certification authorizing the

¹⁴ Even the conclusion that AT&T has had “some kind of intelligence relationship” is conjecture, as the court improperly equates “classified work” with an “intelligence relationship.”

¹⁵ It proves nothing that, according to AT&T merger documents cited in Plaintiffs’ Complaint, AT&T “performs various classified contracts, and thousands of its employees hold government security clearances.” 439 F. Supp. 2d at 992 (ER 323) (citing Compl. ¶ 29 (ER 6-7)). This would be true even if AT&T did nothing more than provide telecommunications services to government defense or intelligence agencies. Dozens, if not hundreds, of companies are government contractors that perform classified work.

assistance.” *Id.* (ER 324) (citing 6/23/06 Tr. at 15-21 (ER 128-34)). On that basis, the court reasoned that AT&T helps when asked to do so and when it believes the request is legal; that AT&T believed any request here was legal; and that AT&T must therefore have participated in the program. *See id.* at 993 (ER 324).

This syllogism is multiply flawed. In the first place, this logical chain assumes that AT&T had been “asked to help.” But that issue could never be litigated because of the government’s state secrets assertion. The district court acknowledged this gap but did nothing to close it. *See id.* (noting the “remaining question . . . whether, in implementing the ‘terrorist surveillance program,’ the government ever requested the assistance of AT&T”).

The court’s logic additionally fails because it treats the statements at oral argument – which were premised *on the facts alleged in the Complaint* – as admissions about facts *in the real world*. Far from conceding that anything in the Complaint was true, AT&T simply argued that, based on Plaintiffs’ allegations, AT&T had certain legal immunities. Even the grammatical formulation of AT&T’s oral argument statement was subjunctive. *See id.* at 992 (ER 324) (“any such assistance *would be legal if*”) (citing 6/23/06 Tr. at 15-21 (ER 128-34)). Moreover, private parties cannot waive the state secrets privilege.¹⁶

¹⁶ *See Reynolds*, 345 U.S. at 7-8 (“The privilege belongs to the Government and must be asserted by it; it can neither be claimed nor waived by a private party.”)

Simply put, at each step along the way, the reasoning the district court employed to conclude that “AT&T and the government have for all practical purposes already disclosed that AT&T assists the government in monitoring communication content,” 439 F. Supp. 2d at 991-92 (ER 323), is deeply flawed. There has been no such disclosure, either by AT&T or by the government, and the district court’s logical leaps, unsupported inferences, and speculation furnish no basis to second-guess the explicit judgment of the Director of National Intelligence that whether AT&T assisted in any program is a state secret.

It is even more clearly the case that the district court’s reasoning does not establish that *AT&T* will be able to litigate this issue fully and fairly. Even if Plaintiffs could adduce non-privileged evidence that they contended would support an inference of participation in the kind of dragnet program they allege, AT&T would be disabled by the state secrets privilege from controverting or contesting Plaintiffs’ evidence. Dismissal is required in such circumstances. *See, e.g., Kasza*, 133 F.3d at 1166; *Halkin I*, 598 F.2d at 11; *Halkin II*, 690 F.2d at 1000.

(footnote omitted). Indeed, the United States may assert the state secrets privilege even in the face of a sworn confession of personal involvement in an intelligence operation. *See Tenet*, 544 U.S. at 6; *Totten*, 92 U.S. 105.

III. PLAINTIFFS CANNOT ESTABLISH STANDING BECAUSE THE STATE SECRETS PRIVILEGE PRECLUDES ADJUDICATION OF WHETHER PLAINTIFFS WERE INJURED BY THE ALLEGED SURVEILLANCE ACTIVITIES

Even if AT&T participated in the activities alleged in the Complaint and such an allegation could be proven, Plaintiffs still would be unable to establish their standing without state secrets. In order to establish injury-in-fact, Plaintiffs must demonstrate that the content or records of *their* communications were intercepted by the NSA. *See supra* pp. 24-25.¹⁷

As detailed below, the United States' invocation of the state secrets privilege prevents this issue from ever being litigated, as that invocation implicates the operational details, including the targets, of the alleged programs at issue here.

A. The State Secrets Privilege Prevents Adjudication of Whether Plaintiffs Were Injured by Alleged Content Surveillance

Plaintiffs cannot establish standing to challenge any of the content surveillance they allege.

As an initial matter, and as discussed above, *see supra* p. 36, Plaintiffs have disclaimed any injury from the targeted surveillance allegedly conducted under the TSP, so there appears to be no live issue here with respect to that program. Even were that not the case, however, the government's assertion of the state secrets

¹⁷ Out of an abundance of caution, AT&T reiterates that it neither confirms nor denies that it is or has been participating in any surveillance program, and nothing in this brief should be interpreted to do so.

privilege would prevent Plaintiffs from demonstrating injury-in-fact under the TSP. Little is known of this program beyond the bare fact of its existence, and the government has not disclosed the identities of the TSP's surveillance targets. The government's limited revelations about the program's general contours are thus insufficient to permit Plaintiffs to demonstrate standing, as they cannot establish (and AT&T cannot rebut) whether their particular communications were accessed by the government without disclosure of information that the government has identified as a state secret.

As noted above, the courts have consistently held that public disclosure of the existence of some aspects of a government intelligence program provides no basis to void the privilege with respect to aspects of the program that have not been disclosed. *See supra* pp. 36-38; *see also Halkin II*, 690 F.2d at 994 (“disclosure of an overseas CIA station's *existence* is a far cry from disclosure of the *activities* carried on by that station”). It is equally well-established that information regarding the particular individuals who were or were not subject to surveillance necessarily reveals the sources/methods of a surveillance program and thus is covered by the state secrets doctrine. *See Halkin I*, 598 F.2d at 8 (concluding that identifying surveillance targets would reveal intelligence methods and techniques and dismissing contrary arguments as “naïve”).

Plaintiffs equally cannot demonstrate injury with respect to AT&T's supposed cooperation with the alleged *untargeted* surveillance of communications content. At no point has the government admitted the existence of such a program. The district court properly recognized that “[t]he existence of this alleged program and AT&T’s involvement, if any, remain far from clear.” 439 F. Supp. 2d at 994-95 (ER 324).

That should have been the end of the matter. The scope and targets of any such alleged program fall squarely within the scope of the United States’ state secrets privilege claim, *see* Negrofonte Decl. ¶ 12 (ER 58-59); Alexander Decl. ¶ 8 (ER 64), and the district court never concluded that this privilege claim could be overridden. Thus, the evidence that would be necessary to allow the court to adjudicate whether any such alleged program actually embraces the communications of all AT&T customers, including Plaintiffs, is unavailable to both sides.

The district court nonetheless found that litigation over Plaintiffs’ standing to challenge this alleged activity could proceed. The court reasoned that Plaintiffs had alleged that *all* AT&T customers and subscribers are subject to this program, *see* 439 F. Supp. 2d at 1000 (ER 331); that the Klein and Marcus declarations furnish “at least some factual basis for plaintiffs’ standing” to challenge such activity, *id.* at 1001 (ER 332); and that, in part because of the government’s

acknowledgment of the TSP, Plaintiffs would be entitled to “receiv[e] at least some evidence tending to establish the factual predicate for the injury-in-fact” arising from this very different claimed program, *id.* at 994, 996-97, 1001 (ER 325, 328, 331). None of these points permits the district court to adjudicate Plaintiffs’ standing to challenge the unconfirmed program of untargeted content surveillance they allege.

1. The Allegations of the Complaint Are Insufficient To Establish Standing

The district court first reasoned that “the gravamen of plaintiffs’ complaint is that AT&T has created a dragnet that collects the content and records of its customers’ communications. The court cannot see how any one plaintiff will have failed to demonstrate injury-in-fact if that plaintiff effectively demonstrates that all class members have so suffered.” 439 F. Supp. 2d at 1000 (ER 331) (citation omitted).

This analysis does not advance the standing inquiry for two reasons. First, the Complaint does not in fact make this allegation. The relevant paragraphs are hedged and do not allege that this program entailed the surveillance of all communications of every AT&T customer or subscriber, regardless of which AT&T facilities route their communications. *See* Compl. ¶ 44 (ER 9) (alleging the acquisition of the “content of all *or a substantial number* of the wire or electronic communications transferred through the AT&T Corp. facilities where [interception

devices] have been installed”) (emphasis added); *see also, e.g., id.* ¶¶ 42, 45 (ER 9) (“all or a substantial number”).

More fundamentally, the state secrets privilege will prevent Plaintiffs from *proving* any such allegations – and, just as important, will prevent AT&T from contesting them. Proving such allegations would require airing the operational details, if any, of what is allegedly an ongoing but unacknowledged program of counterterrorism surveillance, including which facilities, if any, are used in the manner Plaintiffs allege and what, if any, communications are intercepted at those facilities – matters that fall squarely within the government’s state secrets assertion.. Nothing in the district court’s reasoning, or in any of the precedents of this Court or any other federal court, even purports to justify such an extraordinary step. As another court properly recognized in rejecting a similar “dragnet” argument regarding, in that instance, alleged records surveillance:

The thrust of plaintiffs’ claim is that AT&T shares all of its customer telephone records with the government and that as a result, the plaintiffs are among the persons who have suffered and will continue to suffer the harm that flows from such disclosures. . . . The problem in this case, however, is that the state secrets doctrine bars the disclosure of matters that would enable the [plaintiffs] to establish standing in this manner, specifically whether or not AT&T discloses or has disclosed all of its customer records to the government, or whether or not it discloses or has disclosed the named plaintiffs’ records specifically.

Terkel, 441 F. Supp. 2d at 920.

The same is true here. Plaintiffs cannot prove that their own communications were captured in any such program without access to state secrets, and AT&T cannot contest any showing that might be made with non-privileged evidence. Under these circumstances, Plaintiffs cannot establish standing, and their claims based on alleged untargeted content surveillance cannot proceed.

2. The Marcus and Klein Declarations Are Insufficient To Establish Standing, and Their Validity Cannot Be Litigated Without Violating the State Secrets Privilege

The district court also pointed to the Klein and Marcus declarations, suggesting that these declarations meant that Plaintiffs had “at least some factual basis” for their allegations of standing. 439 F. Supp. 2d at 1001 (ER 332). *But see id.* at 990 (ER 322) (earlier declining to rely on these declarations because they are “mere assertions of knowledge by an interested party”). These declarations in no way establish that the parties will be able to litigate standing fully and fairly without impinging on state secrets.

In the first place, whether these declarations provide “at least some factual basis” for standing is not the relevant legal test. Plaintiffs bear the burden of *establishing* standing, *Lujan*, 504 U.S. at 560; *Scott v. Pasadena Unified Sch. Dist.*, 306 F.3d 646, 655 (9th Cir. 2002), which these declarations assuredly do not do. They neither prove that untargeted dragnet surveillance of the kind alleged by

Plaintiffs actually occurred, nor that any such surveillance captured Plaintiffs' communications.

Moreover, these declarations are not evidence from those "indisputably situated to disclose" reliable information about the alleged intelligence activities, 439 F. Supp. 2d at 990 (ER 322), which the district court itself concluded would be necessary in this context. As the government has represented, "Mr. Klein and Marcus never had access to any of the relevant classified information here, and with all respect to them, through no fault or failure of their own, they don't know anything." 6/23/06 Tr. at 76 (ER 189) (Ass't Att'y Gen. Keisler). Both declarations are therefore replete with hearsay, assumptions, and speculation. *See, e.g.,* Marcus Decl. ¶ 120 (ER 105) ("Assuming that AT&T deployed [redacted] Configurations to as many locations as appears to have been the case, it is highly *probable* that all or substantially all of AT&T's traffic to and from other Internet providers anywhere in the United States was diverted.") (emphases added). This evidence is incompetent to establish the injury-in-fact that is necessary to support a finding of standing. *See United Presbyterian Church*, 738 F.2d at 1380; *see also DaimlerChrysler*, 126 S. Ct. at 1866; *ASARCO*, 490 U.S. at 614 (Kennedy, J.). The declarations are also incompetent to effect a waiver of the government's state secrets privilege, because private parties are not in a position to offer authoritative confirmations of clandestine government intelligence activities. *See Reynolds*, 345

U.S. at 7-8 (“The privilege . . . can neither be claimed nor waived by a private party.”) (footnotes omitted).

Even more to the point, the district court erred in relying on these declarations because, as a result of the state secrets privilege, *the assertions contained in them cannot be tested*. The truth of these declarations cannot be assumed. The declarations might contain misperceptions or honest mistakes; they might contain deliberate falsehoods; or they might be based on an incomplete view or inaccurate understanding of the facts. Yet the government’s assertion of the state secrets privilege bars any party, including AT&T, from presenting evidence in response to these declarations. Questions such as whether a secure room really existed, what its purpose was, what information (if any) went into the supposed room, what equipment was in that room, what happened to any such information inside the room, and what role, if any, NSA may have played in operating or controlling it or accessing information it contained would all constitute operational details that fall squarely within the government’s state secrets assertion.

Because “[t]hese questions cannot be resolved or even put in dispute,” *Zuckerbraun*, 935 F.2d at 547, the district court cannot adjudicate Plaintiffs’ standing to challenge the untargeted content surveillance program based on these declarations, and the case should have been dismissed. *See Kasza*, 133 F.3d at 1166 (emphasizing that dismissal is proper where defendants cannot tender

defenses as a result of state secrets invocation); *Halkin I*, 598 F.2d at 11 (affirming dismissal where defendant would not be able to contest “presumptions” urged by plaintiffs; any other result would be “unfair” to defendants); *Halkin II*, 690 F.2d at 1000 (“With no hope of a complete record and adversarial development of the issue, we cannot authorize such inquiry.”); *McDonnell Douglas Corp. v. United States*, 37 Fed. Cl. 270, 285 (Fed. Cl. 1996) (dismissing on state secrets grounds, because “trying this case would lead to an incomplete record” and consequently “rulings by the trial court and consideration by the Federal Circuit on appeal[] would be a sham.”).

Finally, in many respects, these declarations actually undermine the “factual basis” for Plaintiffs’ standing allegations. They do not substantiate blanket surveillance of all AT&T customers’ communications, as the court’s hypothesized injury would require. Although Klein claims he saw AT&T employees with NSA clearances accessing certain Internet network infrastructure, he does not even pretend to know whether the NSA actually intercepted any Internet traffic. Similarly, Marcus merely opines that, if the program works in the manner he infers, “*significant traffic* to and from the plaintiffs . . . would have been *available* for interception.” Marcus Decl. ¶ 108 (ER 102) (emphases added). Whether any of this traffic was actually intercepted Marcus does not say. Moreover, far from claiming that *all* communications were intercepted, Marcus states that certain

categories of communications were not: he indicates that the hypothesized program covered *only* Internet-based service and *not* traditional telephony, *see id.* ¶ 93 (ER 99) (“[n]othing in the documents suggests that conventional telephony traffic was diverted”), and that within the realm of Internet traffic, the assumed program did not include “*on net* traffic – traffic from one AT&T customer to another,” *id.* ¶ 95 (ER 99). Marcus offers no reason, or even speculation, why an alleged intelligence program that was supposedly so massive in scope nonetheless (on his own theory) excluded both telephone content communication and Internet traffic between AT&T customers. In fact, at no time does he even squarely assert that the program exists – every opinion he offers is admitted hypothesis and depends entirely for its accuracy on the Klein declaration. *See id.* ¶ 1 (ER 78). By excluding these categories of communications from the purported “dragnet,” he undermines the allegation that all AT&T customers had their communications intercepted – even assuming the truth of everything in the Klein declaration and the accuracy of all inferences Marcus attempts to draw from it.

3. In Light of the State Secrets Privilege, Discovery Is Not Available

Perhaps recognizing these substantial analytical gaps, the district court held that “the state secrets privilege will not prevent plaintiffs from receiving at least some evidence tending to establish the factual predicate for the injury-in-fact underlying their claims directed at AT&T’s alleged involvement in the monitoring

of communication content.” 439 F. Supp. 2d at 1001 (ER 331). But such discovery could not fill the gap unless it intruded into the realm of state secrets in a manner not even the district court purported to authorize.

The district court in its opinion identified only one piece of evidence Plaintiffs might obtain without impermissibly invading state secrets: the existence of a statutory certification authorizing AT&T to participate in warrantless surveillance. *See id.* (cross-referencing *id.* at 996-97 (ER 328)). This holding is in error, as the United States will explain in its brief. If a certification existed with respect to any alleged surveillance program, its discovery would confirm, at a minimum, AT&T’s alleged participation, which is a core state secret. Indeed, because the district court itself recognized that “[t]he existence of this alleged program and AT&T’s involvement, if any, remain far from clear,” *id.* at 994-95 (ER 325), the privilege remains “absolute” on the district court’s own reasoning, *Kasza*, 133 F.3d at 1166, and no discovery should be permitted. *See El-Masri*, 2007 WL 625130, at *3, *11 (affirming dismissal without discovery to avoid disclosure of state secrets).¹⁸

¹⁸ The only justification the district court offered for permitting discovery was the government’s purported denial that such surveillance was occurring, on the theory that, “if the government has not been truthful, the state secrets privilege should not serve as a shield for its false public statements.” 439 F. Supp. 2d at 996 (ER 326). But just as an acknowledgement of the existence of a program does not remove state secrets protection, *see supra* pp. 36-38, so too a general denial cannot open

But even if the district court were correct that discovery could be had into the existence of a certification, such discovery would be insufficient to establish Plaintiffs' standing. The district court "recognize[d] that uncovering whether and to what extent a certification exists might reveal information about AT&T's assistance to the government that has not been publicly disclosed." 439 F. Supp. 2d at 995 (ER 326).

Even if this discovery were consistent with the state secrets privilege – which it is not – it would be insufficient to establish Plaintiffs' standing. Unless such discovery revealed additional program details, which the district court recognized it could not do, it could not supply the evidence essential for a finding of standing: proof that *these Plaintiffs' communications* were accessed by the government as part of the program they allege.

B. The State Secrets Privilege Prevents Adjudication of Whether Plaintiffs Were Injured by the Alleged Records Program

Finally, Plaintiffs cannot establish their standing to challenge the last category of NSA surveillance activities alleged in the Complaint: the claimed sharing of databases of *records* of calls placed by AT&T subscribers.

the door for inquiry into other matters that the government has identified as state secrets. Indeed, the only way to prove what the government is not doing is to know exactly what it is doing in this area, which would obviously implicate core state secrets.

The district court, like every other court to consider the question, held that the existence of a records program has never been authoritatively confirmed or denied and that the state secrets privilege prevented any discovery into such a program. *See* 439 F. Supp. 2d at 997-98 (ER 329); *see also Terkel*, 441 F. Supp. 2d at 912, 917; *ACLU v. NSA*, 438 F. Supp. 2d 754, 765 (E.D. Mich. 2006). Yet, unlike the other courts that have held this alleged program to be protected by the state secrets privilege, the district court refused to dismiss Plaintiffs' claims. *See* 439 F. Supp. 2d at 997-98 (ER 329). This was error: if the state secrets privilege renders a claim non-justiciable, then it must be dismissed; Article III allows no option to retain jurisdiction in anticipation of possible future developments. *See also DaimlerChrysler*, 126 S. Ct. at 1868 (even if a plaintiff has standing to assert a different claim before the court, Article III requires dismissal of other claim as to which plaintiff lacks standing).

Plaintiffs allege that AT&T participated in a program by which the NSA allegedly gained "direct access" to AT&T's "databases of stored telephone and Internet records," which AT&T maintains in connection with its provision of telecommunications services. Compl. ¶ 51 (ER 10); *see also id.* ¶ 61 (ER 12). The existence of any such intelligence program is a state secret. *See* Negroponte Decl. ¶ 11 (ER 58); Alexander Decl. ¶ 8 (ER 64). As the district court found, "the government has neither confirmed nor denied whether it monitors communication

records and has never publicly disclosed whether [a communication records program] actually exists.” 439 F. Supp. 2d at 997 (ER 328). Because the existence of such a program is a state secret, the district court properly held that no discovery may be had relating to it. *See id.* at 997-98 (ER 329). As a consequence, Plaintiffs cannot establish whether or not a records program of some sort exists, let alone how it operates or whether they were injured by the alleged disclosure of their own records. Because Plaintiffs cannot establish that they have suffered injury-in-fact from a records program, Plaintiffs lack standing to challenge it, and the district court was required to dismiss Plaintiffs’ claims based on such a program.¹⁹

Instead, the court retained jurisdiction, on the theory that “[i]t is conceivable that these entities might disclose, either deliberately or accidentally, other pertinent information about the communication records program as this litigation proceeds.” *Id.* at 997 (ER 329). This theory of jurisdiction-by-future-leak is unprecedented and wrong.²⁰ Once it became clear that Plaintiffs’ standing to challenge the alleged

¹⁹ For example, Count VI of the Complaint is based entirely upon this alleged program and should have been dismissed in its entirety.

²⁰ It also runs afoul of the principle that standing must be established for each claim. The district court seems to have concluded that, notwithstanding the current lack of standing as to claims concerning the alleged communication records program, those claims can survive so long as *other* claims are pending. But the Supreme Court has repeatedly held that “a plaintiff must demonstrate standing for *each claim* he seeks to press.” *DaimlerChrysler*, 126 S. Ct. at 1854 (emphasis

call records program could not be established, dismissal was required. *See Steel Co. v. Citizens for a Better Env't*, 523 U.S. 83, 94 (1998).

To decline to dismiss Plaintiffs' records claims under these circumstances is akin to retaining jurisdiction over an unripe claim. *But see Southern Pac. Transp. Co. v. City of Los Angeles*, 922 F.2d 498, 502 (9th Cir. 1990) (unripe claims must be dismissed). It also fails for the same reasons that the Supreme Court has rejected the doctrine of "hypothetical jurisdiction." *Steel Co.*, 523 U.S. at 94-100. Under that doctrine, courts decided merits issues without first satisfying themselves of their jurisdiction, typically because a merits issue could be decided more easily. *See id.* at 94. The Supreme Court held that approach improper, because without jurisdiction, a court has no power to consider the merits. *See id.*

The approach adopted here is even less permissible. The court retained jurisdiction over non-justiciable claims not to reach the same result by another means – *i.e.*, to dismiss on the merits rather than for lack of jurisdiction – but rather in the speculative anticipation that facts might later develop that would permit a *different* result, *i.e.*, moving forward with litigation. This is improper in any context, but it is particularly inappropriate where state secrets are concerned. To keep alive claims the plaintiff has no current standing to pursue in case a future

added); *accord Friends of the Earth, Inc. v. Laidlaw Env'tl. Servs. (TOC) Inc.*, 528 U.S. 167, 185 (2000).

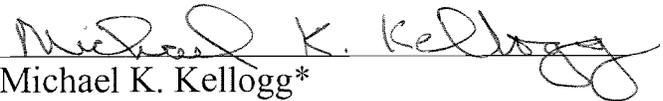
leak of presumed classified information might later allow a finding of jurisdiction is directly at odds with the careful approach the state secrets doctrine demands.

CONCLUSION

The Court should reverse the ruling of the district court and remand with instructions to dismiss Plaintiffs' claims.

Respectfully submitted,

David W. Carpenter
Bradford A. Berenson
Edward R. McNicholas
Eric A. Shumsky
SIDLEY AUSTIN LLP
1501 K Street, N.W.
Washington, D.C. 20005
(202) 736-8000


Michael K. Kellogg*

Sean A. Lev
KELLOGG, HUBER, HANSEN,
TODD, EVANS & FIGEL, P.L.L.C.
1615 M Street, N.W., Suite 400
Washington, D.C. 20036
(202) 326-7900

Bruce A. Ericson
Kevin M. Fong
Marc H. Axelbaum
Jacob R. Sorensen
PILLSBURY WINTHROP SHAW PITTMAN LLP
50 Fremont Street
San Francisco, CA 94105
(415) 983-1000

March 9, 2007

*Counsel of Record

STATEMENT OF RELATED CASES

Defendant-Appellant AT&T Corp. is aware of the following related cases pending in this Court, pursuant to Ninth Circuit Rule 28-2.6, which arises out of the same case in the district court:

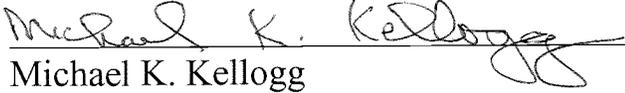
Hepting v. AT&T Corp., No. 06-17137 (9th Cir.)

Al-Haramain Islamic Found. v. Bush, Nos. 06-80134 & 06-36083 (9th Cir.)

**CERTIFICATE OF COMPLIANCE PURSUANT TO
FED. R. APP. P. 32(a)(7)(C) AND CIRCUIT RULE 32-1
FOR CASE NO. 06-17132**

I certify, pursuant to Fed. R. App. P. 32(a)(7)(C) and Circuit Rule 32-1, that the foregoing brief is proportionately spaced, has a typeface of 14 points, and contains 13,751 words.

March 8, 2007


Michael K. Kellogg