

PUBLIC UNCLASSIFIED BRIEF

No. 06-17137

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

TASH HEPTING, et al., Plaintiffs - Appellees,

v.

AT&T CORP., et al., Defendants, and

UNITED STATES OF AMERICA, Intervenor - Appellant.

**ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA**

BRIEF FOR THE UNITED STATES

PAUL D. CLEMENT
Solicitor General

PETER D. KEISLER
Assistant Attorney General

GREGORY G. GARRE
Deputy Solicitor General

DOUGLAS N. LETTER
THOMAS M. BONDY
ANTHONY A. YANG
Attorneys, Appellate Staff
Civil Division, Room 7513
U.S. Department of Justice
950 Pennsylvania Ave., N.W.
Washington, D.C. 20530
Telephone: (202) 514-3602

DARYL JOSEFFER
Assistant to the Solicitor
General

TABLE OF CONTENTS

TABLE OF AUTHORITIES iii

STATEMENT OF JURISDICTION 1

STATEMENT OF ISSUES 2

STATEMENT OF THE CASE 2

STATEMENT OF FACTS 3

 I. The Terrorist Surveillance Program 3

 II. Plaintiffs’ Suit And The State Secrets Privilege Assertion 5

 III. The District Court’s Order 8

 IV. The FISA Court’s January 10, 2007 Orders 9

SUMMARY OF ARGUMENT 10

STANDARD OF REVIEW 14

ARGUMENT 15

 I. THE STATE SECRETS DOCTRINE REQUIRES DISMISSAL
 IF THE VERY SUBJECT MATTER OF A CASE IS A STATE
 SECRET, OR IF PLAINTIFFS CANNOT ESTABLISH A
 PRIMA FACIE CASE OR DEFENDANTS CANNOT MOUNT
 A DEFENSE WITHOUT STATE SECRETS 15

 II. THE VERY SUBJECT MATTER OF THIS CASE IS A STATE
 SECRET 16

 A. Plaintiffs’ Suit Is Premised On An Alleged Secret
 Espionage Relationship 16

 B. The District Court’s Error In Refusing To Dismiss
 This Case Is Compounded By Its Treatment Of
 Plaintiffs’ Communications Records Claims. 25

III. PLAINTIFFS’ STANDING CANNOT BE ESTABLISHED OR REFUTED ABSENT RECOURSE TO STATE SECRETS.	26
A. Plaintiffs Cannot Establish Standing Because The State Secrets Privilege Forecloses Litigation Over Whether They Have Been Subject To Surveillance.	28
B. Plaintiffs Cannot Establish Standing On The Basis Of A “Dragnet” Theory	32
IV. THE STATE SECRETS PRIVILEGE ALSO PRECLUDES LITIGATION OF THE MERITS OF PLAINTIFFS’ CLAIMS	37
A. Fourth And First Amendments	37
B. FISA And Other Statutes	41
C. [REDACTED TEXT]	46
CONCLUSION	47
STATEMENT OF RELATED CASES	
ADDENDUM	
CERTIFICATE OF COMPLIANCE	
CERTIFICATE OF SERVICE	

TABLE OF AUTHORITIES

Cases:

<i>ACLU v. NSA</i> , 438 F. Supp. 2d 754 (E.D. Mich. 2006), appeal pending, Nos. 06-2095, 06-2140 (6th Cir.)	25
<i>Bareford v. General Dynamics Corp.</i> , 973 F.2d 1138 (5th Cir. 1992)	21
<i>Board of Educ. v. Earls</i> , 536 U.S. 822 (2002)	40
<i>CIA v. Sims</i> , 471 U.S. 159 (1985)	24
<i>Chicago & S. Air Lines v. Waterman S.S. Corp.</i> , 333 U.S. 103 (1948)	41
<i>City of Indianapolis v. Edmond</i> , 531 U.S. 32 (2000)	40
<i>City of Los Angeles v. Lyons</i> , 461 U.S. 95 (1983)	43
<i>DaimlerChrysler Corp. v. Cuno</i> , 126 S. Ct. 1854 (2006)	27, 33
<i>Director, Office of Workers' Comp. Programs v. Newport News Shipbuilding & Dry Dock Co.</i> , 514 U.S. 122 (1995)	30
<i>Edmonds v. Department of Justice</i> , 323 F. Supp. 2d 65 (D.D.C. 2004)	26
<i>El-Masri v. United States</i> , ___ F.3d ___, 2007 WL 625130 (4th Cir. Mar. 2, 2007)	15, 19, 20, 21

<i>Ellsberg v. Mitchell</i> (“ <i>Ellsberg I</i> ”), 709 F.2d 51 (D.C. Cir. 1983)	15, 16, 28, 36
<i>Ellsberg v. Mitchell</i> (“ <i>Ellsberg II</i> ”), 807 F.2d 204 (D.C. Cir. 1986)	35
<i>Gest v. Bradbury</i> , 443 F.3d 1177 (9th Cir. 2006)	44
<i>Halkin v. Helms</i> (“ <i>Halkin I</i> ”), 598 F.2d 1 (D.C. Cir. 1978)	15
<i>Halkin v. Helms</i> (“ <i>Halkin II</i> ”), 690 F.2d 977 (D.C. Cir. 1982)	28, 39
<i>Hamilton v. Dillin</i> , 88 U.S. 73 (1874)	41
<i>Hayden v. National Security Agency</i> , 608 F.2d 1381 (D.C. Cir. 1979)	23
<i>Illinois v. McArthur</i> , 531 U.S. 326 (2001)	37, 38
<i>Kasza v. Browner</i> , 133 F.3d 1159 (9th Cir. 1998)	6, 15, 16, 21, 35
<i>Laird v. Tatum</i> , 408 U.S. 1 (1972)	29
<i>Linder v. National Security Agency</i> , 94 F.3d 693 (D.C. Cir. 1996)	24
<i>Lujan v. Defenders of Wildlife</i> , 504 U.S. 555 (1992)	26, 27
<i>MacWade v. Kelly</i> , 460 F.3d 260 (2d Cir. 2006)	40

<i>Ex parte Milligan</i> , 71 U.S. 2 (1866)	41
<i>Morrison v. Olson</i> , 487 U.S. 654 (1988)	42
<i>National Treasury Employees Union v. Von Rabb</i> (“NTEU”), 489 U.S. 656 (1989)	38, 39, 40
<i>Samson v. California</i> , 126 S. Ct. 2193 (2006)	37
<i>In re Sealed Case</i> , 310 F.3d 717 (FIS Ct. of Rev. 2002)	38, 42
<i>Smelt v. County of Orange</i> , 447 F.3d 673 (9th Cir. 2006)	27
<i>Sterling v. Tenet</i> , 416 F.3d 338 (4th Cir. 2005)	26, 35
<i>Tenenbaum v. Simonini</i> , 372 F.3d 776 (6th Cir. 2004)	16
<i>Tenet v. Doe</i> , 544 U.S. 1 (2005)	6, 11, 12, 16, 17, 18, 19, 20
<i>Terkel v. AT&T Corp.</i> , 441 F. Supp. 2d 899 (N.D. Ill. 2006)	25
<i>Totten v. United States</i> , 92 U.S. 105 (1875)	6, 11, 12, 15, 16, 17, 18, 19, 20, 41
<i>United States ex rel. Ross v. LaVallee</i> , 341 F.2d 823 (2d Cir. 1965)	30
<i>United States v. Brown</i> , 484 F.2d 418 (5th Cir. 1973)	38, 39

<i>United States v. Buck</i> , 548 F.2d 871 (9th Cir. 1977)	38
<i>United States v. Butenko</i> , 494 F.2d 593 (3d Cir. 1974)	38, 39
<i>United States v. Curtiss-Wright Export Corp.</i> , 299 U.S. 304 (1936)	42
<i>United States v. Marchetti</i> , 466 F.2d 1309 (4th Cir. 1972)	15
<i>United States v. Navarro-Vargas</i> , 408 F.3d 1184 (9th Cir. 2005)	35
<i>United States v. Nixon</i> , 418 U.S. 683 (1974)	15
<i>United States v. Ott</i> , 827 F.2d 473 (9th Cir. 1987)	29
<i>United States v. Reynolds</i> , 345 U.S. 1 (1953)	6, 15, 21, 35, 46
<i>United States v. Sweeny</i> , 157 U.S. 281 (1895)	42
<i>United States v. Truong</i> , 629 F.2d 908 (4th Cir. 1980)	38, 39
<i>United States v. U.S. District Court (“Keith”)</i> , 407 U.S. 297 (1972)	38
<i>Warth v. Seldin</i> , 422 U.S. 490 (1975)	27
<i>Weinberger v. Catholic Action of Hawaii/Peace Educ. Project</i> , 454 U.S. 139 (1981)	19

<i>Weston v. Lockheed Missiles & Space Co.</i> , 881 F.2d 814 (9th Cir. 1989)	16
<i>Youngstown Sheet & Tube Co. v. Sawyer</i> , 343 U.S. 579 (1952)	42

U.S. Constitution:

Article II	15
Section 2	42
Article III	26, 27
Amendment I	29, 37, 40
Amendment IV	28, 29, 37, 38, 39, 40
Clause 1	37

Statutes:

Authorization for Use of Military Force (“AUMF”), Pub. L. No. 107-40, 115 Stat. 224 (2001)	4, 42
Preamble	42
Section 2(a)	42
Communications Act of 1947, as amended	
47 U.S.C. 222	46
47 U.S.C. 605	30
47 U.S.C. 605(a)	30, 45
47 U.S.C. 605(e)(3)(A)	30

Foreign Intelligence Surveillance Act of 1978 (“FISA”), as amended, 50 U.S.C. 1801-1871	5, 41
50 U.S.C. 1801(f)	29, 41
50 U.S.C. 1801(k)	29
50 U.S.C. 1809(a)	41
50 U.S.C. 1810	29
National Security Agency Act of 1959, Pub. L. No. 86-36, 73 Stat. 63 (1959)	23
Section 6 (50 U.S.C. § 402 note)	23
Pen Register Act of 1986, as amended, 18 U.S.C. 3121-3127	
18 U.S.C. 3121	46
Stored Communication Act of 1986, as amended, 18 U.S.C. 2701-2712	
18 U.S.C. 2702(a)	30, 44
18 U.S.C. 2702(b)(2)	45
18 U.S.C. 2703(e)	45
18 U.S.C. 2707(a)	30
18 U.S.C. 2707(e)	45
18 U.S.C. 2711(1)	30
Title III, Omnibus Crime Control and Safe Streets Act of 1968, as amended, 18 U.S.C. 2510-2520	30, 44, 45
18 U.S.C. 2510(11)	30
18 U.S.C. 2511	44
18 U.S.C. 2511(2)(a)(ii)	45
18 U.S.C. 2518(7)	45
18 U.S.C. 2520(a)	30

28 U.S.C. 1292(b)	2
28 U.S.C. 1331	1
28 U.S.C. 1332	1
28 U.S.C. 1367	1
28 U.S.C. 2201	1
50 U.S.C. § 403-1(i)(1)	24

Regulations:

Proclamation No. 7463, 66 Fed. Reg. 48,199 (Sept. 14, 2001)	3
--	---

Legislative Materials:

H.R. Rep. No. 95-1283 (1978)	29
------------------------------------	----

Miscellaneous:

President's News Conference, 41 Weekly Comp. Pres. Doc. 1885 (Dec. 19, 2005)	4
---	---

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

No. 06-17137

**TASH HEPTING, et al.,
Plaintiffs - Appellees,**

v.

**AT&T CORP., et al.,
Defendants,**

and

**UNITED STATES OF AMERICA,
Intervenor - Appellant.**

**ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA**

BRIEF FOR THE UNITED STATES

STATEMENT OF JURISDICTION

Plaintiffs filed this action against AT&T Corp., et al. ("AT&T"), on January 31, 2006, invoking the district court's jurisdiction under 28 U.S.C. 1331, 1332, 1367, and 2201. Excerpts of Record ("ER") 3. The United States intervened and moved to dismiss because the state secrets privilege precludes disclosure of information necessary to adjudicate the case. On July 20, 2006, the district court issued an order

declining to dismiss the case and certifying its order for immediate appeal under 28 U.S.C. 1292(b). On November 7, 2006, this Court granted petitions for interlocutory appeal by the United States and AT&T. ER 340.

STATEMENT OF ISSUES

Plaintiffs contend that “[t]his case challenges the legality of [AT&T’s] participation in a *secret* and illegal government program to intercept and analyze vast quantities of Americans’ telephone and Internet communications.” ER 2 ¶2 (emphasis added). This appeal presents the question whether the district court erred in declining to dismiss this case, even though:

(1) the suit’s very subject matter—including the relationship, if any, between AT&T and the Government in connection with the secret intelligence activities alleged by plaintiffs—is a state secret;

(2) plaintiffs’ standing cannot be established or refuted absent disclosure of state secrets; and

(3) the state secrets privilege precludes litigation of the merits of plaintiffs’ claims.

STATEMENT OF THE CASE

Plaintiffs allege that AT&T has collaborated in secret National Security Agency (“NSA”) foreign intelligence gathering activities, including the Terrorist Surveillance Program (“TSP”) that the President established in the aftermath of the

September 11, 2001 attacks. The President and his top national security advisors deemed the TSP essential to protecting against future terrorist attacks, and the TSP proved critical to detecting and disrupting al Qaeda plots during the ongoing conflict. Plaintiffs also allege that AT&T has participated in a broader program, never acknowledged by the United States, purportedly surveilling “millions of ordinary Americans.” ER 3 ¶7.

The United States intervened, formally invoked the state secrets privilege, and moved to dismiss because this case cannot be litigated without recourse to highly classified state secrets concerning foreign intelligence gathering. The district court rejected the argument that the state secrets privilege requires dismissal, denied the motions to dismiss, and *sua sponte* certified its order for interlocutory appeal. ER 236, 308.

STATEMENT OF FACTS

I. The Terrorist Surveillance Program.

On September 11, 2001, al Qaeda agents who had entered the United States launched coordinated attacks on key strategic sites, killing approximately 3,000 people—the highest single-day death toll from foreign attacks in the Nation’s history. The President immediately declared a national emergency in view of “the continuing and immediate threat of further attacks on the United States.” 66 Fed. Reg. 48,199 (2001). The United States also launched a military campaign against al Qaeda, and

Congress authorized the President “to use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks” of September 11. See Authorization for Use of Military Force (“AUMF”), Pub. L. No. 107-40, § 2(a), 115 Stat. 224 (2001). The Nation’s armed forces remain engaged in a global conflict against the al Qaeda terrorist network.

The September 11 attacks demonstrated the ability of al Qaeda operatives to infiltrate the United States and murder Americans. Top al Qaeda leaders, including Osama bin Laden, have repeatedly vowed to strike America and her allies again. As the President has explained, “[t]he terrorists want to strike America again, and they hope to inflict even greater damage than they did on September the 11th.” President’s News Conference, 41 Weekly Comp. Pres. Doc. 1885, 1886 (Dec. 19, 2005).

Against this backdrop, and in light of unauthorized media disclosures, the President acknowledged in December 2005, that he had authorized the TSP by directing NSA to intercept international communications into and out of the United States of persons linked to al Qaeda. See *id.* at 1885. The Government publicly stated that communications would be intercepted under this program only if there were reasonable grounds to believe that one party to the communication was a member or agent of al Qaeda or an affiliated terrorist organization. See *id.* at 1889;

ER 47, 50. The Government has never revealed the methods and means of the TSP, because of the grave harm to national security that would result from such disclosure.

As discussed below, the President recently determined not to reauthorize the TSP in view of orders issued by the Foreign Intelligence Surveillance Court on January 10, 2007.

II. Plaintiffs' Suit And The State Secrets Privilege Assertion.

A. Plaintiffs filed this action against AT&T, alleging that “[i]n December 2005, the press revealed that the government had instituted a comprehensive and warrantless electronic surveillance program.” ER 2 ¶3. According to plaintiffs, “[t]his surveillance program, purportedly authorized by the President at least as early as 2001 and primarily undertaken by the National Security Agency without judicial review or approval, intercepts and analyzes the communications of millions of Americans” (*ibid.*; see ER 7-9), and, “[o]n information and belief,” AT&T “has opened its key telecommunications facilities and databases to direct access by the NSA,” thus “disclosing to the government the contents of its customers’ communications as well as detailed communications records” (ER 3 ¶6; see ER 9-10). Plaintiffs claimed that the alleged surveillance violated the Foreign Intelligence Surveillance Act (“FISA”), 50 U.S.C. 1801 *et seq.*, and assorted other statutes, and sought monetary, declaratory, and injunctive relief. See ER 29-31.

The United States intervened, formally asserted the state secrets privilege and related statutory privileges through the then-Director of National Intelligence, John Negroponte, and the NSA's Director, General Keith Alexander, and moved to dismiss or, in the alternative, for summary judgment. We argued that dismissal was required under *Tenet v. Doe*, 544 U.S. 1 (2005), and *Totten v. United States*, 92 U.S. 105 (1875), because plaintiffs' case is premised on an asserted secret espionage relationship between the United States and AT&T that cannot be litigated.

We also explained that the state secrets privilege requires dismissal whenever "there is a reasonable danger" that disclosing information in court proceedings would harm national security interests, such as by disclosing intelligence-gathering methods or capabilities. See *Kasza v. Browner*, 133 F.3d 1159, 1166 (9th Cir. 1998). That privilege, which must be invoked personally by the pertinent agency head, requires dismissal of a case if the "very subject matter" of the action is a state secret, or if the plaintiff cannot prove a *prima facie* case, or the defendant cannot establish a valid defense, without information protected by the privilege. See *id.* at 1166; *United States v. Reynolds*, 345 U.S. 1 (1953).

Director Negroponte and General Alexander explained in public declarations that to discuss the underlying activities here in any greater detail than had been made public by the Government

would disclose classified intelligence information and reveal intelligence sources and methods, which would enable adversaries of the United States to avoid detection by the U.S. Intelligence Community and/or take measures to defeat or neutralize U.S. intelligence collection, posing a serious threat of damage to the United States' national security interests.

ER 58 ¶11; see ER 63 ¶7. With respect to plaintiffs' allegations regarding AT&T's purported involvement with NSA, Director Negroponte and General Alexander elaborated that

[t]he United States can neither confirm nor deny allegations concerning intelligence activities, sources, methods, relationships, or targets. * * * The only recourse for the Intelligence Community and, in this case, for the NSA is to neither confirm nor deny these sorts of allegations, regardless of whether they are true or false. To say otherwise when challenged in litigation would result in routine exposure of intelligence information, sources, and methods and would severely undermine surveillance activities[.]

ER 58-59 ¶12; see ER 64 ¶8. The Government also provided the district court with *ex parte, in camera* classified declarations from Director Negroponte and General Alexander discussing plaintiffs' allegations and pertinent facts, as well as the Government's assertion of the state secrets privilege.

B. [REDACTED TEXT—PUBLIC TEXT CONTINUES ON PAGE 8]

III. The District Court's Order.

A. On July 20, 2006, the district court denied the Government's motion for dismissal or summary judgment, as well as AT&T's motion to dismiss. Regarding plaintiffs' allegations regarding communications *contents*, the court first decided that AT&T's alleged involvement with NSA in a secret surveillance program cannot be a state secret. Noting that the Government had "publicly admitted the existence of" the TSP, the court stated that "it is inconceivable that this program could exist without the acquiescence and cooperation of some telecommunications provider." ER 323. For the same reasons, the court concluded that "the very subject matter of this action is hardly a secret [because] public disclosures by the government and AT&T indicate that AT&T is assisting the government to implement some kind of surveillance program." ER 325.

The court declined to resolve the Government's argument that plaintiffs cannot demonstrate their standing to sue because the state secrets privilege prevents them from establishing actual injury. The court ruled that the privilege does not bar plaintiffs from seeking discovery of evidence concerning AT&T's alleged participation in communications content monitoring. ER 331.

The court further "decline[d] to decide at this time whether this case should be dismissed on the ground that the government's state secrets assertion will preclude evidence necessary for plaintiffs to establish a *prima facie* case or for AT&T to raise

a valid defense to the claims.” ER 325. According to the court, “[p]laintiffs appear to be entitled to at least some discovery,” and “[b]ecause of the public disclosures by the government and AT&T, the court cannot conclude that merely maintaining this action creates a ‘reasonable danger’ of harming national security.” *Ibid.*

B. The court also refused to dismiss plaintiffs’ allegations concerning communications *records*. The court agreed with the Government and AT&T that no activities regarding communications records had been confirmed or denied by the United States, and the court thus refused to permit any discovery. ER 328-29. It nevertheless declined to dismiss these claims, reasoning that “[i]t is conceivable” that the Government or telecommunications providers “might disclose, either deliberately or accidentally, other pertinent information about the communication records program as this litigation proceeds.” ER 329.

IV. The FISA Court’s January 10, 2007 Orders.

While this appeal was pending, the Attorney General publicly advised the Senate Judiciary Committee that, “on January 10, 2007, a Judge of the Foreign Intelligence Surveillance Court issued orders authorizing 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. As a result of these orders, any electronic surveillance that was occurring as part of the Terrorist Surveillance

Program will now be conducted subject to the approval of the Foreign Intelligence Surveillance Court.” ER 341.

The Attorney General explained that, while “the [TSP] fully complies with the law,” the “complex” and “innovative” FISA Court orders “will allow the necessary speed and agility while providing substantial advantages” for conducting foreign intelligence activities. *Ibid.* “[U]nder these circumstances, the President has determined not to reauthorize the Terrorist Surveillance Program when the current authorization expires.” ER 341-42.

The Government subsequently submitted to the district court public and classified declarations of General Alexander discussing the January 10 FISA Court orders. See ER 347 (public version).

SUMMARY OF ARGUMENT

The President and his top national security advisors determined that the TSP was necessary to protect the Nation from further attack by an enemy that already inflicted the deadliest foreign attack ever on American soil and that has vowed to strike again. Whether AT&T is involved in either the TSP or the broader activities alleged by plaintiffs is a state secret that neither the Government nor AT&T can confirm or deny. Litigating even plaintiffs’ standing, let alone the merits of their claims, would reveal extraordinarily sensitive intelligence information that, if

disclosed, would cause the Nation grievous injury. The district court therefore erred in permitting this action to proceed.

I. Plaintiffs' suit is premised on their allegation that AT&T has assisted the Government in conducting secret foreign intelligence gathering activities. Because plaintiffs' entire action rests upon alleged secret espionage activities, including an alleged secret espionage relationship between AT&T and the Government concerning the alleged activities, this suit must be dismissed now as a matter of law. The Supreme Court has settled that a case premised on the existence of an alleged secret espionage relationship cannot be maintained. See *Tenet*, 544 U.S. 1; *Totten*, 92 U.S. 105. Moreover, the Government has formally invoked the state secrets privilege, and the public and classified declarations of the Director of National Intelligence and the Director of NSA make clear that disclosure of any information tending to confirm or deny alleged secret surveillance activities, including any relationship between AT&T and the Government in connection with such alleged activities, would pose a grave threat to national security. That assertion of the state secrets privilege independently compels dismissal of plaintiffs' lawsuit.

In declining to dismiss this action, the district court reasoned that the Government had publicly disclosed the existence of the TSP, and that, in the court's view, it is unclear whether such a program could have existed without AT&T's cooperation. On that basis, the court speculated that AT&T must have been involved

in the surveillance activities at issue. That speculation was fundamentally misplaced. The Government has *never* divulged whether or to what extent AT&T was or was not involved in *any* way in the TSP or in any other alleged activities. Nor has the Government disclosed the methods and means of the TSP, or whether any alleged secret activities beyond the TSP ever existed. The district court overstepped its authority in disregarding the assessments of the National Intelligence and NSA Directors that confirmation or denial of such facts would undermine the Nation's security.

The fact that the Government has disclosed the *existence* of the TSP does not preclude dismissal, just as the well-known fact that the Government had a secret spy program during the Civil War (*Totten*) and the Cold War (*Tenet*) did not preclude dismissal in *Totten* and *Tenet*. The methods and means of the TSP's operation have never been divulged, but instead remain secret and highly classified. As Director Negroponte and General Alexander explained, confirmation or denial of secret surveillance activities in litigation "would result in routine exposure of intelligence information, sources, and methods and would severely undermine surveillance activities in general." ER 59.

The court's error in refusing to dismiss this case is underscored by its treatment of plaintiffs' communications records claim. The court *agreed* with the Government and AT&T that no activity of any kind with respect to communications records has

ever been disclosed, and correctly determined that no discovery could be allowed. The court nevertheless declined to dismiss the claim, ruling that there might be future disclosures, perhaps inadvertent, that would make such matters no longer secret. This was manifest error. A court may not refuse to dismiss a claim subject to a proper invocation of the state secrets privilege simply because the possibility remains—in part because of the existence of the litigation—that damaging disclosures could ensue. Such a rule would improperly invite disclosures harmful to national security.

II. Dismissal of this case is also required because the state secrets privilege precludes plaintiffs from establishing, and defendants from refuting, their threshold standing to sue. Plaintiffs claim that AT&T has assisted the Government in connection with unlawful surveillance, but they do not and cannot show that their own communications have been intercepted. Because the state secrets privilege protects from disclosure any information tending (among other things) to confirm or deny the subjects of surveillance, the question whether any particular plaintiff has suffered injury as a result of the alleged surveillance cannot be litigated.

Nor is there any merit to the district court's theory that plaintiffs can establish standing here because anyone who is an AT&T customer can claim injury. That theory rests upon improper speculation concerning the nature and scope of the activities at issue. Even plaintiffs do not allege that all communications of AT&T customers are intercepted, and, in any event, they could not show that in light of the

state secrets privilege. As the Government has made clear, the TSP targeted only international communications of persons associated with al Qaeda or related terrorist organizations. Plaintiffs cannot meet their burden of showing actual injury due to the complained-of activity, nor could such a showing be rebutted in light of the state secrets privilege.

III. Dismissal of this case is likewise compelled because the state secrets privilege forecloses adjudication of the merits of plaintiffs' claims. Litigation of any of plaintiffs' claims would necessarily entail detailed exploration of the nature and scope of, and the reasons for, the Government's underlying intelligence activities, and of the relationship, if any, between AT&T and the Government in connection with such activities. As explained in the public and classified declarations, any consideration of those matters would be barred under the state secrets privilege.

STANDARD OF REVIEW

This appeal raises questions of law reviewable *de novo*.

ARGUMENT

I. THE STATE SECRETS DOCTRINE REQUIRES DISMISSAL IF THE VERY SUBJECT MATTER OF A CASE IS A STATE SECRET, OR IF PLAINTIFFS CANNOT ESTABLISH A PRIMA FACIE CASE OR DEFENDANTS CANNOT MOUNT A DEFENSE WITHOUT STATE SECRETS.

The Executive's ability to protect military or state secrets from disclosure has been recognized as vital from the beginning of the Republic. See *Totten*, 92 U.S. at 106-07; *Reynolds*, 345 U.S. at 6-7. Because “[g]athering intelligence information” is “within the President’s constitutional responsibility for the security of the Nation as the Chief Executive and as Commander in Chief of our Armed forces” (*United States v. Marchetti*, 466 F.2d 1309, 1315 (4th Cir. 1972)), the state secrets privilege derives from the President’s Article II powers to conduct foreign affairs and provide for the national defense. *United States v. Nixon*, 418 U.S. 683, 710 (1974); *El-Masri v. United States*, ___ F.3d ___, 2007 WL 625130, at *4 (4th Cir. Mar. 2, 2007).

“[T]he privilege to protect state secrets must head the list” of governmental privileges. *Halkin v. Helms*, 598 F.2d 1, 7 (D.C. Cir. 1978) (“*Halkin I*”). It covers sensitive information when litigation would result in “disclosure of intelligence-gathering methods or capabilities.” *Ellsberg v. Mitchell*, 709 F.2d 51, 57 (D.C. Cir. 1983) (“*Ellsberg I*”). The privilege also protects information that may appear innocuous on its face, but which in a larger context could reveal sensitive classified information. See *Kasza*, 133 F.3d at 1166; *Halkin I*, 598 F.2d at 8.

An assertion of the state secrets privilege by a federal agency head must be “accorded the ‘utmost deference’ and the court’s review of the privilege claim is narrow.” *Kasza*, 133 F.3d at 1166. The courts must honor its assertion whenever “a reasonable danger exists that disclosing the information in court proceedings would harm national security interests.” *Tenenbaum v. Simonini*, 372 F.3d 776, 777 (6th Cir. 2004). “When properly invoked, the state secrets privilege is absolute. No competing public or private interest can be advanced to compel disclosure of information found to be protected by a claim of privilege.” *Ellsberg I*, 709 F.2d at 57; see *Weston v. Lockheed Missiles & Space Co.*, 881 F.2d 814, 816 (9th Cir. 1989).

If the “very subject matter” of the action is a state secret, the case must be dismissed. See *Tenet*, 544 U.S. at 8-9; *Totten*, 92 U.S. at 106-07; *Kasza*, 133 F.3d at 1166. Similarly, if “the plaintiff cannot prove the *prima facie* elements of her claim with nonprivileged evidence,” or the privilege “deprives the *defendant* of information that would otherwise give the defendant a valid defense to the claim,” the case must be dismissed. *Kasza*, 133 F.3d at 1166.

II. THE VERY SUBJECT MATTER OF THIS CASE IS A STATE SECRET.

A. Plaintiffs’ Suit Is Premised On An Alleged Secret Espionage Relationship.

1. According to plaintiffs’ own complaint, “[t]his case challenges the legality of Defendants’ participation in a *secret* and illegal government program.” ER 2 ¶2

(emphasis added). That allegation puts this case squarely within the *Totten/Tenet* rule of dismissal. The critical premise of the complaint is that AT&T has been collaborating with NSA in a “secret” (*ibid.*) and “classified surveillance program” (ER 7 ¶32).

The Supreme Court held in *Totten* and *Tenet* that—wholly aside from the assertion of the state secrets privilege—a case must be dismissed where, as here, it necessarily depends on an alleged secret espionage agreement with the Government. In *Totten*, the Supreme Court affirmed the dismissal at the outset of an action seeking to enforce an alleged espionage contract for services rendered during the Civil War, reasoning that “public policy forbids the maintenance of any suit in a court of justice, the trial of which would inevitably lead to the disclosure of matters which the law itself regards as confidential.” *Totten*, 92 U.S. at 107. In *Tenet*, the Supreme Court reaffirmed *Totten*, again directing dismissal of a suit to enforce an alleged secret espionage agreement, and reiterating that “*Totten* precludes judicial review in cases such as respondents’ where success depends upon the existence of their secret espionage relationship with the Government.” *Tenet*, 544 U.S. at 8.

The holding and reasoning of *Totten* and *Tenet* are directly applicable here. As noted, plaintiffs allege that AT&T has been and is assisting NSA in connection with a “secret” surveillance program. See, e.g., ER 2-3 ¶¶2, 3, 7. And plaintiffs claim that this secret program has harmed them and is unlawful. Just as in *Tenet*, plaintiffs’

“success” in this lawsuit thus “depends upon the existence” of a “secret espionage relationship with the Government.” *Tenet*, 544 U.S. at 8. Whether and to what extent such a relationship exists has never been disclosed, and, as the Supreme Court has instructed, “public policy forbids the maintenance of any suit in a court of justice, the trial of which would inevitably lead to the disclosure of matters which the law itself regards as confidential.” *Totten*, 92 U.S. at 107.

The district court recognized that “this case involves an alleged covert relationship between the government and AT&T,” but it nevertheless held that *Totten* and *Tenet* pose no bar because “[t]he implicit notion in *Totten* was one of equitable estoppel: one who agrees to conduct covert operations impliedly agrees not to reveal the agreement even if the agreement is breached.” ER 322-23. In the court’s view, because “AT&T, the alleged spy, is not the plaintiff here,” plaintiffs have “made no agreement with the government and are not bound by any implied covenant of secrecy.” *Ibid.*

This reasoning fundamentally misreads *Totten* and *Tenet*, neither of which turned on an “implicit” equitable estoppel theory. Rather, the Supreme Court explained explicitly that “*Totten*’s core concern” lies in “preventing the existence of [an alleged spy’s] relationship with the Government from being revealed” (*Tenet*, 544 U.S. at 10), and accordingly, “lawsuits premised on alleged espionage agreements are altogether forbidden” (*id.* at 9). Disclosure would cause the same harm to national

security regardless of whether the plaintiff was a party to an alleged relationship. Because plaintiffs' action hinges on the existence of an asserted secret espionage relationship between AT&T and NSA, *Totten* and *Tenet* are directly applicable.

Weinberger v. Catholic Action of Hawaii/Peace Educ. Project, 454 U.S. 139 (1981)—cited by the Supreme Court in *Tenet*, 544 U.S. at 9—confirms the error of the district court's "implicit" equitable estoppel theory. There, the Supreme Court invoked *Totten* in dismissing a challenge under the National Environmental Protection Act ("NEPA"), where the determination whether the Navy complied with NEPA would "inevitably lead to the disclosure of matters which the law itself regards as confidential." 454 U.S. at 147 (quoting *Totten*, 92 U.S. at 107). Thus, the Supreme Court in *Weinberger* applied the *Totten* rule completely outside the context of an asserted espionage agreement, and precluded a lawsuit by someone with no contractual relationship with the Government. *Weinberger* thus underscores that *Totten* is not a rule of "equitable estoppel."

The Fourth Circuit's recent ruling in *El-Masri* is also instructive. There, as in this case, the plaintiff sued corporate and individual defendants, alleging their participation in secret and unlawful Government activity (extraordinary rendition). The Fourth Circuit affirmed dismissal of the case on state secrets grounds, explaining that, for the litigation to proceed, plaintiff "would have to demonstrate the existence and details of [Government] espionage contracts, an endeavor practically

indistinguishable from that categorically barred by *Totten* and *Tenet*.” *El-Masri*, ___ F.3d at ___, 2007 WL 625130 at *9. That analysis applies equally here.

2. The district court also reasoned that, “unlike the clandestine spy arrangements in *Tenet* and *Totten*, AT&T and the government have for all practical purposes already disclosed that AT&T assists the government in monitoring communication content.” ER 323. The court explained that the Government has disclosed the existence of the TSP, and, according to the court, it was “unclear whether this program could even exist without AT&T’s acquiescence and cooperation,” considering “the ubiquity of AT&T telecommunications services” and the fact that “AT&T’s history of cooperating with the government on such matters is well known.” *Ibid*.

This logic is fundamentally flawed. As discussed, the Supreme Court has directed the dismissal of cases at the outset because their very subject matter was a secret, even though the existence of the program at issue was publicly known. Indeed, in *Totten* and *Tenet* themselves, it was obviously well known that the Government employed spies in both the Civil War and the Cold War, and the existence of the Government program for relocating spies was known in *Tenet*, 544 U.S. at 4 n.2, but the crux of the Supreme Court’s decisions was that the details of such activities were to remain secret and were not a permissible topic of litigation. Here, although the Government has disclosed the *existence* of the TSP, the methods

and means of the TSP's operation remain closely guarded and highly classified secrets. See ER 59 ¶12, 64 ¶8; accord *El-Masri*, ___ F.3d at ___, 2007 WL 625130 at *8-11.

Furthermore, in reasoning that AT&T's participation with NSA had "for all practical purposes" already been disclosed, ER 323, the court erred in considering not only official Government statements, but also statements of AT&T and other telecommunications providers. As the Supreme Court has admonished, the state secrets privilege "belongs to the Government" and cannot be "waived by a private party." *Reynolds*, 345 U.S. at 7; see *Kasza*, 133 F.3d at 1165. Thus, in inquiring whether a relationship had been confirmed or denied, the district court should have limited itself to authoritative Government statements, and should not have looked to statements by other persons or entities. As the courts have recognized, "disclosure of information by government officials can be prejudicial to government interests, even if the information has already been divulged from non-government sources." *Bareford v. General Dynamics Corp.*, 973 F.2d 1138, 1144 (5th Cir. 1992).

Even if it had been proper to consider AT&T's statements, none of the links in the district court's speculative chain of inferences withstands scrutiny. The court's initial premise—that NSA could not conduct the alleged activities without the assistance of the private sector (ER 323)—has no foundation in the public record, and the court cited none. The court also focused on the fact that AT&T is a large

company (*ibid.*), but the court had absolutely no basis for supposing that only large firms, and not small ones, would have the resources or expertise to furnish any needed assistance (if, indeed, there has been any such assistance). Similarly, the fact that AT&T has a history of providing some assistance to the Government, including on some unspecified classified contracts (see ER 7 ¶¶29, 323), does not mean that the Government requested AT&T's assistance, or that AT&T provided assistance, with respect to *the NSA surveillance activities alleged in this case*.

Indeed, even considering AT&T's general statements concerning its cooperation with the United States on unspecified projects, no relationship between AT&T and NSA in connection with any of the alleged activities here has *ever* been disclosed, and the public record provides no basis for inferring whether such a relationship exists. The district court was thus able to state only that "AT&T is assisting the government to implement *some kind* of surveillance program," and "AT&T and the government have *some kind* of intelligence relationship," ER 325-26 (emphasis added), conclusions that surely are not sufficient to override the judgment of the Director of National Intelligence on a matter of national security. The district court plainly erred in arrogating to itself the determination whether confirmation of the court's speculation concerning AT&T's involvement in the alleged activities would harm national security.

As Director Negroponete and General Alexander stressed, the “United States can neither confirm nor deny allegations concerning intelligence activities, sources, methods, relationships, or targets.” ER 58-59 ¶12; see ER 64 ¶8. Significantly, this is “[t]he only recourse” for the Government “regardless of whether [the allegations] are true or false,” because “[t]o say otherwise * * * would result in routine exposure of intelligence information, sources, and methods and would severely undermine surveillance activities.” ER 58-59 ¶12. Thus, “any further elaboration in the public record concerning these matters would reveal information that could cause the very harms [that] assertion of the state secrets privilege is intended to prevent.” *Ibid.*; see ER 64 ¶8. The district court had no proper basis, and cited none, for disagreeing with the assessments—set out more comprehensively in the classified declarations—from the Nation’s top-level intelligence officials.

The district court also overlooked that Congress itself has determined that NSA’s “‘unique and sensitive’ activities” require “‘extreme security measures.’” *Hayden v. National Security Agency*, 608 F.2d 1381, 1390 (D.C. Cir. 1979). Section 6 of the National Security Agency Act of 1959 provides in explicit terms that “nothing in this Act or any other law * * * shall be construed to require the disclosure of the organization or any function of the National Security Agency, [or] of any information with respect to the activities thereof.” See Pub. L. No. 86-36, § 6, 73 Stat. 63, 64 (50 U.S.C. § 402 note). “The protection afforded by section 6 is, by its

very terms, absolute.” *Linder v. National Security Agency*, 94 F.3d 693, 698 (D.C. Cir. 1996). Congress has also vested the Director of National Intelligence with authority and responsibility to “protect intelligence sources and methods from unauthorized disclosure,” 50 U.S.C. § 403-1(i)(1), a “sweeping” recognition that “[i]t is the responsibility of the Director * * * to weigh the variety of complex and subtle factors in determining whether disclosure of information may lead to an unacceptable risk of compromising the * * * intelligence-gathering process.” *CIA v. Sims*, 471 U.S. 159, 169, 180 (1985). These statutory privileges bearing upon the NSA’s activities reinforce the conclusion that the state secrets privilege requires dismissal here, and provide an additional, independent basis for that conclusion.

[REDACTED TEXT—PUBLIC TEXT CONTINUES ON PAGE 25]

B. The District Court's Error In Refusing To Dismiss This Case Is Compounded By Its Treatment Of Plaintiffs' Communications Records Claims.

The district court's refusal to dismiss plaintiffs' claims regarding an alleged program of monitoring communications *records* is equally flawed. Indeed, every other court to have addressed the issue has dismissed such claims. See *Terkel v. AT&T Corp.*, 441 F. Supp. 2d 899 (N.D. Ill. 2006) (dismissing communications records claim on state secrets grounds); *ACLU v. NSA*, 438 F. Supp. 2d 754, 765 (E.D. Mich. 2006) (same with respect to "data mining" claim), *appeal pending*, Nos. 06-2095/2140 (6th Cir.).

With respect to plaintiffs' allegations regarding communications records, the court *agreed* with the Government and AT&T that no such activities had been confirmed or denied, and the court thus refused to permit any discovery, but it nevertheless declined to dismiss those claims. ER 328-29. The court reasoned that "[i]t is conceivable that [the Government or telecommunications providers] might disclose, either deliberately or accidentally, other pertinent information about the communication records program as this litigation proceeds," and, if so, "such disclosures might make this program's existence or non-existence no longer a secret." ER 329; see also ER 331-32.

Neither law nor logic supports that approach to subverting protection of state secrets. The state secrets privilege requires dismissal in order to *protect* state secrets;

it does not permit courts to keep cases alive on the off chance that there may be deliberate or accidental disclosures of such secrets. “Courts are not required to play with fire and chance further disclosure—inadvertent, mistaken, or even intentional—that would defeat the very purpose for which the privilege exists.” *Sterling v. Tenet*, 416 F.3d 338, 344 (4th Cir. 2005); see *Edmonds v. Department of Justice*, 323 F. Supp. 2d 65, 81-82 (D.D.C. 2004). The courts may not invite such harm to national security by denying or deferring a valid assertion of the state secrets privilege.

III. PLAINTIFFS’ STANDING CANNOT BE ESTABLISHED OR REFUTED ABSENT RECOURSE TO STATE SECRETS.

Even if the very subject matter of this suit were not a state secret, dismissal would be required because plaintiffs cannot establish standing, and AT&T cannot refute plaintiffs’ standing, without recourse to information protected by the state secrets privilege. The Constitution “limits the jurisdiction of federal courts to ‘Cases’ and ‘Controversies,’” and “the core component of standing is an essential and unchanging part of th[is] case-or-controversy requirement.” *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 559-60 (1992). To have Article III standing, a plaintiff must establish three elements—injury, causation, and redressability—and each element must not only be alleged, but proven. See *id.* at 560-61. To meet the injury requirement, a plaintiff must show that he suffered an injury in fact to a “legally

protected interest” that is “concrete and particularized” and “actual or imminent, not ‘conjectural’ or ‘hypothetical.’” *Id.* at 560.

A plaintiff must demonstrate Article III standing for “each claim he seeks to press,” *DaimlerChrysler Corp. v. Cuno*, 126 S. Ct. 1854, 1867 (2006), and must further establish “prudential” standing by showing that “the constitutional or statutory provision on which [each] claim rests properly can be understood as granting persons in the plaintiff’s position a right to judicial relief.” *Warth v. Seldin*, 422 U.S. 490, 499-500 (1975). To do so, a plaintiff normally “must assert his own legal rights and interests, and cannot rest his claim to relief on the legal rights or interests of third parties.” *Smelt v. County of Orange*, 447 F.3d 673, 682 (9th Cir. 2006). To advance a statutory claim, a plaintiff must show that his particular injury “fall[s] within ‘the zone of interests to be protected or regulated by the statute’” in question. *Id.* at 683.

Here, the state secrets privilege prevents plaintiffs from establishing, and defendants from refuting, any injury because it bars proof of whether plaintiffs’ communications have been subject to surveillance. Accordingly, both Article III and prudential standing requirements dictate dismissal of plaintiffs’ case.

A. Plaintiffs Cannot Establish Standing Because The State Secrets Privilege Forecloses Litigation Over Whether They Have Been Subject To Surveillance.

Courts have refused to recognize standing to challenge a Government surveillance program where the state secrets privilege prevents a plaintiff from establishing, and the Government from refuting, that he was actually subject to surveillance. For example, in *Halkin v. Helms*, 690 F.2d 977 (D.C. Cir. 1982) (“*Halkin II*”), as here, plaintiffs claimed that Government surveillance and interception of their communications violated the Fourth Amendment in a case in which the state secrets privilege barred litigation over whether plaintiffs’ communications were actually intercepted. Plaintiffs thus relied on the claim that their names were included on “watchlists” used to govern NSA surveillance, and they argued that this fact demonstrated a “substantial threat” that their communications would be intercepted. See *id.* at 983-84, 997. The D.C. Circuit nevertheless affirmed dismissal of the Fourth Amendment claim, “hold[ing] that appellants’ inability to adduce proof of actual acquisition of their communications” rendered them “incapable of making the showing necessary to establish their standing to seek relief.” *Id.* at 998. As here, plaintiffs “alleged, but ultimately cannot show, a concrete injury” in light of the Government’s invocation of the state secrets privilege. *Id.* at 999.

Like *Halkin* and the present case, *Ellsberg v. Mitchell*, 709 F.2d 51 (D.C. Cir. 1983), also involved a challenge to Government surveillance where the Government

invoked the state secrets privilege. The D.C. Circuit again held that dismissal was warranted where a plaintiff could not, absent recourse to state secrets, establish that he was actually subject to surveillance. As the court explained, “[a]n essential element of each plaintiff’s case is proof that he himself has been injured. Membership in a group of people, ‘one or more’ members of which were exposed to surveillance, is insufficient to satisfy that requirement.” *Id.* at 65.^{1/}

Analogous standing principles apply to plaintiffs’ statutory claims. FISA authorizes only an “aggrieved person” to bring a civil action challenging the acquisition of communications contents. 50 U.S.C. 1801(f), 1810. To ensure that this term would be “coextensive [with], but no broader than, those persons who have standing to raise claims under the Fourth Amendment with respect to electronic surveillance” (H.R. Rep. No. 95-1283, at 66 (1978)), Congress defined “aggrieved person” to mean one “whose communications or activities were *subject to* electronic surveillance” or who was *targeted* by such surveillance. 50 U.S.C. 1801(k) (emphasis added). Litigants who cannot establish their status as “aggrieved persons” therefore do “not have standing” under “any” of FISA’s provisions. H.R. Rep. No. 95-1283, at 89-90; cf. *United States v. Ott*, 827 F.2d 473, 475 n.1 (9th Cir. 1987); see

^{1/} Similarly, any chill of expressive activity resulting from fear that a surveillance program may cause harm in the future cannot establish a non-speculative injury that might confer standing to bring plaintiffs’ First Amendment claim. See *Laird v. Tatum*, 408 U.S. 1, 11, 13-14 (1972).

also *Director, Office of Workers' Comp. Programs v. Newport News Shipbuilding & Dry Dock Co.*, 514 U.S. 122, 126 (1995) (“aggrieved” is a well-known term of art used “to designate those who have standing”).

Title III similarly specifies that civil actions may be brought by a “person whose * * * communication *is* intercepted, disclosed, or intentionally used.” 18 U.S.C. 2520(a) (emphasis added). The Stored Communications Act likewise limits its civil remedies to “person[s] aggrieved” under that statute, see 18 U.S.C. 2707(a), and the only persons aggrieved by a communication-service provider’s “knowing[] divulge[nce]” of the “contents of a communication” or of customer records, 18 U.S.C. 2702(a), are those persons whose communications or records were actually divulged. See 18 U.S.C. 2711(1) (adopting § 2510(11) definition of “aggrieved person” as one “who was a party to any intercepted * * * communication” or “a person against whom the interception was directed”). Plaintiffs additionally seek relief under 47 U.S.C. 605, but this statute makes equally clear that only a “person aggrieved” may challenge allegedly unlawful “divulge[nce] or publi[cation]” of the contents of a communication, see 47 U.S.C. 605(a), (e)(3)(A), and “only a party to a tapped conversation may complain” of an alleged disclosure under § 605. See *United States ex rel. Ross v. LaVallee*, 341 F.2d 823, 824 (2d Cir. 1965).

Each of these provisions reflects the fundamental point that only persons whose rights were injured by the actual interception or disclosure of their own

communications (or records) have standing. Because the state secrets privilege precludes plaintiffs from attempting to demonstrate, and defendants from attempting to dispute, that plaintiffs' own communications have been intercepted (see ER 58-59 ¶12, 64 ¶8), litigation over plaintiffs' standing is foreclosed.

[REDACTED TEXT—PUBLIC TEXT CONTINUES ON PAGE 32]

**B. Plaintiffs Cannot Establish Standing On The Basis Of
A “Dragnet” Theory.**

The district court believed that this fatal problem could be circumvented because plaintiffs allege a “dragnet” created by AT&T to “intercept all or substantially all of its customers’ communications,” and that, if this were proven, “all” of AT&T’s customers (including the four plaintiffs here) would have had their communications intercepted and, thus, would have suffered a “concrete injury” sufficient to establish standing. ER 331. As the court recognized, however, plaintiffs “allege a surveillance program of far greater scope than the publicly disclosed [‘TSP’],” and the “existence of [such an undisclosed] program and AT&T’s involvement, if any, remain far from clear.” ER 325. But those mere allegations are insufficient to justify the district court’s denial of our motion to dismiss because any discovery or litigation concerning the existence of that alleged broader program would necessarily delve into what surveillance activities the Government has actually undertaken, an inquiry foreclosed by the state secrets privilege. See ER 58 ¶12.

Even assuming *arguendo* that AT&T assisted the Government in implementing the TSP and that such a hypothetical relationship were not itself a state secret, plaintiffs have only two options for challenging AT&T’s alleged assistance: (1) they must attempt to challenge alleged TSP surveillance based on the Government’s limited public disclosures; or (2) they must attempt to challenge some alleged

surveillance activity *different from* TSP surveillance. Either way, plaintiffs cannot establish standing, because they cannot show that *they* were subject to the TSP, nor can they show that any broader program ever existed, much less intercepted their communications. The Supreme Court's reminder last term in *DaimlerChrysler* that standing must exist and be established independently for each claim is fatal to plaintiffs' case. To the extent they challenge the TSP, status as an AT&T customer clearly does not suffice. To the extent they challenge a hypothetical broader "dragnet," the suit is clearly barred by the state secrets privilege, because, as noted, any discovery or litigation concerning that matter would necessarily probe the Government's intelligence operations, thereby infringing upon privileged information.

If plaintiffs seek to challenge AT&T's alleged participation in the TSP's focused collection of one-end-foreign communications involving al Qaeda, they have alleged nothing to support the claim that their own communications have been intercepted. The Attorney General has publicly explained that TSP surveillance was governed by "strict guidelines" because the President's authorization directed the NSA "*only* to engage in surveillance of [certain international] communications" where there were reasonable grounds "to conclude that one of the parties of the communication [was] either a member of al Qaeda or affiliated with al Qaeda." ER 47 (emphasis added). The district court likewise recognized that the President

publicly stated that the TSP “strictly target[ed] al Qaeda and their known affiliates.” ER 320; see also ER 50. The Government specifically invoked the state secrets privilege to protect from disclosure any information describing “this activity in any greater detail,” in part to protect the efficacy of surveillance now conducted subject to the approval of the FISA Court. ER 58 ¶11 (Negroponte); see *id.* ¶12; ER 63-64 ¶¶7-8 (Alexander).

Plaintiffs here have not alleged that they were targets of TSP surveillance, or that they have communicated with persons who were targets. See ER 4 ¶¶13-16, 14 ¶70, 16 ¶74. In fact, they *disclaim* any such allegation. See ER 14 ¶70. Instead, the district court based its standing determination on the very different theory that *all* of AT&T’s customers (including plaintiffs) suffered injury because of AT&T’s alleged participation in a so-called content “dragnet” far broader than the TSP. See ER 325, 331. But because plaintiffs cannot establish the existence of any such broader surveillance program, the allegation of the existence of such a program does not establish standing.

The district court concluded that the Government had “opened the door for judicial inquiry” into the scope of the TSP by denying TSP surveillance beyond that targeting one-end-foreign communications of members or agents of al Qaeda and related terrorist organizations. ER 328. That conclusion is flawed on multiple levels. Plaintiffs’ “dragnet” theory challenges a purported secret program *other than and*

broader than the TSP, an activity which the Government has never acknowledged. Even under the district court's reasoning, such a challenge to an entirely unconfirmed program cannot proceed to discovery; that is why the district court denied discovery concerning plaintiffs' communications records claims. See pp. 25-26, *supra*.

To the extent plaintiffs' suit is seen as challenging the veracity of the Government's public acknowledgment of the *TSP* itself, that challenge is insufficient to overcome the "presumption of regularity and good faith" given to official acts of Executive Branch officials, *United States v. Navarro-Vargas*, 408 F.3d 1184, 1207 (9th Cir. 2005) (en banc). That presumption is particularly strong in the state secrets context because the privilege is invoked by the "head" of an Executive Branch department based on "actual personal consideration," *Reynolds*, 345 U.S. at 8. As noted, courts must afford the Government's assertion of the state secrets privilege "utmost deference," and the judiciary's "narrow" role is to determine whether there is "reasonable danger" that compulsion of the evidence at issue could harm national security, "without forcing disclosure of the very thing the privilege is designed to protect." See *Kasza*, 133 F.3d at 1165-66. Courts accordingly cannot allow litigants "to force 'groundless fishing expeditions' upon them," *Sterling*, 416 F.3d at 344, and a plaintiff is not permitted to "embark on a fishing expedition in government waters on the basis of [its own] speculation," *Ellsberg v. Mitchell*, 807 F.2d 204, 207-08 (D.C. Cir. 1986) (Scalia, Circuit Justice) ("*Ellsberg II*").

Even plaintiffs' allegations confirm that the state secrets privilege requires dismissal. Plaintiffs contend that AT&T "installed and used" devices in certain key AT&T facilities "for use in the [NSA's Surveillance] Program," and that these devices acquire content and non-content information regarding "all or a substantial number" of the communications that pass through those particular facilities. ER 7 ¶¶32, 9-10 ¶¶43-47. Because these allegations fall short of contending, much less proving, that the communications of *all* AT&T customers were intercepted, plaintiffs must still demonstrate that their own communications were intercepted. See *Ellsberg I*, 709 F.2d at 65 (standing cannot be established by proving "[m]embership in a group of people, 'one or more' members of which were exposed to surveillance"). Such a showing would necessarily require evidence revealing the targets of surveillance, information that falls within the heartland of the state secrets privilege. See ER 58-59 ¶12, 64 ¶8. And, even assuming that plaintiffs' general allegations concerning AT&T's installation and use of devices were accurate, the inquiry required to determine how those devices operated, and what communications were intercepted, would expose the operational details of any such surveillance, and, accordingly, would improperly reveal intelligence sources and methods squarely protected by the privilege. See *ibid*.

[REDACTED TEXT—PUBLIC TEXT CONTINUES ON PAGE 37]

IV. THE STATE SECRETS PRIVILEGE ALSO PRECLUDES LITIGATION OF THE MERITS OF PLAINTIFFS' CLAIMS.

Even if the very subject matter of this litigation were not a state secret, and even if plaintiffs could prove their standing, this case should have been dismissed for an independent reason: plaintiffs cannot prove the elements of their claims, and AT&T could not defend itself against such claims, without resort to state secrets.

A. Fourth And First Amendments.

Plaintiffs' constitutional claims are barred by the state secrets privilege. The Fourth Amendment provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." U.S. Const. amend. IV, cl. 1. The Amendment's "central requirement" is thus one of "reasonableness." *Illinois v. McArthur*, 531 U.S. 326, 330 (2001). Reasonableness is determined by assessing "the degree to which [the search] intrudes upon an individual's privacy" and the "degree to which it is needed for the promotion of legitimate governmental interests" in the context of the "totality of the circumstances" surrounding the search. See *Samson v. California*, 126 S. Ct. 2193, 2197 (2006). Because this reasonableness inquiry depends on the nature of the search and the circumstances surrounding it, the Supreme Court has repeatedly explained that "neither a warrant, nor probable cause, nor, indeed, any measure of individualized suspicion, is an indispensable component of reasonableness in every

circumstance.” *National Treasury Employees Union v. Von Rabb*, 489 U.S. 656, 665 (1989) (“*NTEU*”); see *McArthur*, 531 U.S. at 330.

With respect to the TSP, at least two different exceptions to the warrant requirement are satisfied: the President’s inherent authority to conduct warrantless surveillance of foreign powers, and the Fourth Amendment’s “special needs” doctrine. The President has inherent constitutional authority, notwithstanding the Fourth Amendment, to conduct warrantless surveillance of communications involving foreign powers such as al Qaeda and its agents. While the Supreme Court has expressly reserved that question, *United States v. U.S. District Court*, 407 U.S. 297, 308, 321-22 & n.20 (1972), every court of appeals that has since decided it has held that the President possesses “inherent authority” under the Constitution, not trumped by the Fourth Amendment, “to conduct warrantless searches to obtain foreign intelligence information.” *In re Sealed Case*, 310 F.3d 717, 742 & n.26 (FIS Ct. of Rev. 2002); accord *United States v. Buck*, 548 F.2d 871, 875-76 (9th Cir. 1977); *United States v. Truong*, 629 F.2d 908, 912-17 (4th Cir. 1980); *United States v. Butenko*, 494 F.2d 593, 602-06 (3d Cir. 1974); *United States v. Brown*, 484 F.2d 418, 425-26 (5th Cir. 1973). Indeed, this proposition is now so firmly entrenched that the Foreign Intelligence Surveillance Court of Review—the appellate tribunal charged with reviewing FISA Court decisions—took “for granted that the President does have that authority.” *In re Sealed Case*, 310 F.3d at 742.

Under the foreign intelligence doctrine, warrantless searches are reasonable if conducted to secure foreign intelligence information. See *Truong*, 629 F.2d at 916-17; *Butenko*, 494 F.2d at 606; *Brown*, 484 F.2d at 421, 425. Inquiry into the facts surrounding a decision to conduct TSP surveillance, however, would necessarily confront the state secrets privilege. As discussed, facts concerning the program’s “intelligence activities, sources, methods, relationships, or targets” can neither be confirmed nor denied. ER 58-59 ¶¶11-12. The D.C. Circuit concluded in analogous circumstances that the “notion of deciding [the] constitutional question” of “whether a warrant is required in certain foreign intelligence surveillances, and if not, whether certain activities are ‘reasonable’” when the “record [is] devoid of any details that might serve even to identify the alleged victim of a violation,” is not only “impossible,” but “ludicrous.” *Halkin II*, 690 F.2d at 1000, 1003 n.96.

The “special needs” doctrine independently supports the validity of the TSP. “[W]here a Fourth Amendment intrusion serves special governmental needs, beyond the normal need for law enforcement, it is necessary to balance the individual’s privacy expectations against the Government’s interests to determine whether it is impractical to require a warrant or some level of individualized suspicion in the particular context.” *NTEU*, 489 U.S. at 665-66. The “special needs” doctrine applies in “a variety of contexts,” including warrantless searches used to detect and prevent drunk driving, drug use by students and federal officials, airline hijackings, and

terrorist bombings. See *MacWade v. Kelly*, 460 F.3d 260, 263, 268 (2d Cir. 2006); *Board of Educ. v. Earls*, 536 U.S. 822, 835-36 (2002); *City of Indianapolis v. Edmond*, 531 U.S. 32, 44 (2000). It is “settled” that the Government’s need to “discover” and “prevent the development of hazardous conditions” can qualify as a special need justifying warrantless and suspicionless searches. See *NTEU*, 489 U.S. at 668.

In applying the “special needs” doctrine, reasonableness is determined by conducting a “fact-specific balancing” of the Government interests underlying the search and the associated intrusion into privacy interests. See *Earls*, 536 U.S. at 830. Again, the state secrets privilege protects the information required in this case for this fact-specific inquiry, such as information concerning the nature of the al Qaeda threat; facts supporting the need for speed and flexibility in conducting surveillance beyond that traditionally available under the FISA; details concerning the TSP’s targeting decisions, effectiveness in detecting and preventing terrorist attacks, and other operational information; and other specifics concerning the scope and nature of TSP surveillance. See ER 58-59 ¶¶11-12, 63-64 ¶¶7-8. Application of the special needs doctrine therefore cannot properly be adjudicated in light of the state secrets privilege. Nor is there any basis to suppose that plaintiffs’ First Amendment claim is any less fact-dependent than their Fourth Amendment claim.

B. FISA And Other Statutes.

1. Plaintiffs' statutory claims fare no better. Plaintiffs allege violation of FISA, see ER 19-20, which occurs if a person "intentionally—(1) engages in electronic surveillance under color of law except as authorized by statute; or (2) discloses or uses information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance not authorized by statute." 50 U.S.C. 1809(a). Even if plaintiffs could show that the TSP's activities qualified as "electronic surveillance" (see 50 U.S.C. 1801(f)), and otherwise fell within the scope of FISA, their claim that FISA precluded TSP surveillance, thereby constraining the President's ability to collect surveillance of a foreign enemy during wartime, raises a grave constitutional question, the proper resolution of which would necessarily require consideration of matters protected by the state secrets privilege.

In wartime, the "President alone" is "constitutionally invested with the entire charge of hostile operations." *Hamilton v. Dillin*, 88 U.S. 73, 87 (1874). Congress may not "interfere[] with the command of the forces and the conduct of campaigns" as that "power and duty belong to the President as commander-in-chief." *Ex parte Milligan*, 71 U.S. 2, 139 (1866) (Chase, C.J., concurring). The President's Commander-in-Chief powers include secretly gathering intelligence information about foreign enemies. See, e.g., *Totten*, 92 U.S. at 106; *Chicago & S. Air Lines v.*

Waterman S.S. Corp., 333 U.S. 103, 111 (1948); *United States v. Curtiss-Wright Export Corp.*, 299 U.S. 304, 320 (1936). As discussed, every court of appeals to have decided the question has held that, even in peacetime, the President has inherent constitutional authority to conduct warrantless surveillance of foreign powers within or without the United States. The Foreign Intelligence Surveillance Court of Review thus “t[ook] for granted” that the President had such authority and that “FISA could not encroach on the President’s constitutional power.” *In re Sealed Case*, 310 F.3d at 742.^{2/}

Congress may not “impede the President’s ability to perform his constitutional duty.” *Morrison v. Olson*, 487 U.S. 654, 691 (1988); see *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 637-38 (1952) (Jackson, J., concurring). The Constitution designates the President as Commander-in-Chief, U.S. Const., art. II, § 2, and “the object of the [Commander-in-Chief Clause] is evidently to vest in the [P]resident * * * such supreme and undivided command as would be necessary to the prosecution of a successful war.” *United States v. Sweeny*, 157 U.S. 281, 284 (1895). In the context of the current conflict with al Qaeda—a foreign enemy that has already

^{2/} In the context of this case, the President’s constitutional prerogative to engage in surveillance directed at al Qaeda is reinforced by Congress’s Authorization for Use of Military Force (see p. 4, *supra*), which recognized the President’s “authority under the Constitution to take action to deter and prevent acts of international terrorism against the United States,” and explicitly authorized the President to act against those responsible for the attacks of September 11, 2001. See AUMF pmb., § 2(a).

attacked the United States—the President and his top advisors determined that the threat to the United States demanded that signals intelligence be carried out with a speed and methodology that could not be achieved by seeking judicial approval through the traditional FISA process (but which is now occurring subject to the recent, innovative orders of the FISA Court).

For present purposes, the crucial point is that the constitutionality of any limits placed on the President’s authority to gather foreign intelligence against the enemy in wartime cannot be measured without a precise understanding of the program at issue and the need for that program. That inquiry would require careful consideration of the nature and scope of the surveillance in question, as well as the precise nature of the existing al Qaeda threat, including an examination of the scope, targets, methods, and means of surveillance directed against that threat. As discussed above, the facts relevant to that inquiry are protected from disclosure by the state secrets privilege, which requires dismissal of plaintiffs’ claim.^{3/}

^{3/} Similarly, to the extent that plaintiffs would seek to invoke the new FISA Court orders as part of an attack on the TSP, the nature and content of those orders would also implicate state secrets. We note as well that the new orders highlight that plaintiffs’ claims for prospective equitable relief concerning the TSP (as opposed to damages for past surveillance) suffer an additional jurisdictional defect: the TSP no longer exists. Whether viewed as a question of standing or mootness, “[p]ast exposure to illegal conduct does not in itself show a present case or controversy regarding injunctive [or declaratory] relief if unaccompanied by any continuing, present adverse effects.” *City of Los Angeles v. Lyons*, 461 U.S. 95, 102 (1983).
(continued...)

2. Litigation of plaintiffs' remaining statutory claims is also barred by the state secrets privilege. Plaintiffs allege violation of 18 U.S.C. 2511 (Title III), which generally proscribes the intentional interception of wire, oral, or electronic communications, as well as the intentional disclosure or use of the contents of any such communication. See ER 21-22. Similarly, plaintiffs allege violation of 18 U.S.C. 2702(a)(1) and (a)(2) (the Stored Communications Act), which forbid providers of an electronic communication or remote computer service from knowingly divulging the contents of communications stored, carried, or maintained on that service. See ER 24-25. Plaintiffs likewise allege violation of 18 U.S.C. 2702(a)(3), which mandates that "a provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber or customer of such service * * * to any governmental entity." *Ibid.*

^{3/} (...continued)

Thus, plaintiffs must "demonstrate that they are 'realistically threatened by a *repetition* of the [alleged] violation.'" *Gest v. Bradbury*, 443 F.3d 1177, 1181 (9th Cir. 2006). Here, plaintiffs are unable to show any ongoing effects from the TSP because, in light of the FISA Court's January 2007 orders, "any electronic surveillance that was conducted as part of the TSP is now being conducted subject to the approval of the FISA Court." ER 349 ¶3; see ER 341. TSP surveillance is no longer authorized by the President or conducted by NSA, and, accordingly, plaintiffs cannot show that prospective relief would redress any ongoing injury. Because plaintiffs seek only prospective equitable relief for their constitutional claims, ER 13 ¶66, 18 ¶89, 29-30 ¶¶A-B, those claims must be dismissed in their entirety for this additional reason.

Significantly, all of these provisions are subject to 18 U.S.C. 2511(2)(a)(ii), which states that there is no violation where there is a court order or “a certification in writing” by “the Attorney General of the United States that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required.” See 18 U.S.C. 2702(b)(2), 2703(e). Plaintiffs’ claim under 47 U.S.C. 605(a) (ER 23-24), is similarly subject an exception for authorized under Title III. Furthermore, the Stored Communications Act provides that “good faith reliance” on a Government request for interception under 18 U.S.C. 2518(7) is “a complete defense to any civil * * * action brought under [the Act] or any other law.” 18 U.S.C. 2707(e).

Under all of these provisions, plaintiffs fail to state a claim on their merits insofar as AT&T may have been provided with a certification or other legal authorization for an activity in question, and, as we have shown, the state secrets privilege would prevent the existence of any such certification or authorization, or of any secret relationship at all with AT&T, from being confirmed or denied in this litigation. See ER 58-59 ¶¶11-12, 63-64 ¶¶7-8. The district court was thus fundamentally mistaken in positing that “AT&T could confirm or deny the existence of a certification authorizing monitoring of communication content through a combination of responses to interrogatories and *in camera* review by the court.” ER 328. Discovery on this matter is foreclosed, because revealing whether a certification

has issued necessarily bears on whether and to what extent AT&T has had a relationship with the Government in connection with the alleged activities. Nor does *in camera* review resolve the problem: Courts must “not jeopardize the security which the privilege is meant to protect by insisting upon an examination of the evidence, even by the judge alone, in chambers.” *Reynolds*, 345 U.S. at 10.^{4/}

C. [REDACTED TEXT—PUBLIC TEXT CONTINUES ON PAGE 47]

^{4/} For similar reasons, plaintiffs’ claims under 18 U.S.C. 3121, 47 U.S.C. 222, and California unlawful business proscriptions (ER 27-29) cannot be litigated in light of the state secrets privilege.

CONCLUSION

For the foregoing reasons, the district court's decision should be reversed and this case dismissed.

Respectfully submitted,

PAUL D. CLEMENT
Solicitor General

GREGORY G. GARRE
Deputy Solicitor General

DARYL JOSEFFER
Assistant to the Solicitor
General

PETER D. KEISLER
Assistant Attorney General

DOUGLAS N. LETTER
THOMAS M. BONDY
ANTHONY A. YANG
Attorneys, Appellate Staff
Civil Division, Room 7513
U.S. Department of Justice
950 Pennsylvania Ave., N.W.
Washington, D.C. 20530
Telephone: (202) 514-3602

Douglas N. Letter
Thomas M. Bondy
Anthony A. Yang

MARCH 2007

STATEMENT OF RELATED CASES

Hepting v. AT&T Corp., No. 06-17132 (9th Cir.) is AT&T's appeal from the same district court order that is the subject of the present appeal by the Government.

Al-Haramain Islamic Foundation, Inc. v. Bush, No. 06-36083 (9th Cir.), also involves related issues. In that case, this Court granted the Government's petition for immediate appeal under 28 U.S.C. 1292(b), and subsequently granted the Government's motion to hold the appeal in abeyance pending resolution of this appeal (No. 06-17137) and No. 06-17132.

ADDENDUM

ADDENDUM TABLE OF CONTENTS

	<u>Page</u>
Foreign Intelligence Surveillance Act of 1978, as amended,	
50 U.S.C. 1801-1871	1a
50 U.S.C. 1801	1a
50 U.S.C. 1809	2a
50 U.S.C. 1810	2a
Title III, Omnibus Crime Control and Safe Streets Act of 1968, as amended,	
18 U.S.C. 2510-2520	3a
18 U.S.C. 2510	3a
18 U.S.C. 2511	4a
18 U.S.C. 2518	6a
18 U.S.C. 2520	7a
Stored Communication Act of 1986, as amended,	
18 U.S.C. 2701-2712	8a
18 U.S.C. 2702	8a
18 U.S.C. 2703	9a
18 U.S.C. 2707	9a
18 U.S.C. 2711	10a
Pen Register Act of 1986, as amended,	
18 U.S.C. 3121-3127	11a
18 U.S.C. 3121	11a
18 U.S.C. 3127	11a
Communications Act of 1934, as amended	12a
47 U.S.C. 222	12a
47 U.S.C. 605	13a

Foreign Intelligence Surveillance Act of 1978, as amended
50 U.S.C. 1801-1871

50 U.S.C. 1801

§ 1801. Definitions

As used in this subchapter:

* * * *

(f) “Electronic surveillance” means--

(1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;

(2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States, but does not include the acquisition of those communications of computer trespassers that would be permissible under section 2511(2)(i) of Title 18;

(3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or

(4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

* * * *

(k) "Aggrieved person" means a person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance.

* * * *

50 U.S.C. 1809

§ 1809. Criminal sanctions

(a) Prohibited activities

A person is guilty of an offense if he intentionally--

- (1) engages in electronic surveillance under color of law except as authorized by statute; or
- (2) discloses or uses information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance not authorized by statute.

* * * *

50 U.S.C. 1810

§ 1810. Civil liability

An aggrieved person, other than a foreign power or an agent of a foreign power, as defined in section 1801(a) or (b)(1)(A) of this title, respectively, who has been subjected to an electronic surveillance or about whom information obtained by electronic surveillance of such person has been disclosed or used in violation of section 1809 of this title shall have a cause of action against any person who committed such violation and shall be entitled to recover--

- (a) actual damages, but not less than liquidated damages of \$1,000 or \$100 per day for each day of violation, whichever is greater;
- (b) punitive damages; and
- (c) reasonable attorney's fees and other investigation and litigation costs reasonably incurred.

**Title III, Omnibus Crime Control and Safe Streets Act of 1968, as amended
18 U.S.C. 2510-2520**

18 U.S.C. 2510

§ 2510. Definitions

As used in this chapter--

* * * *

(4) "intercept" means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.

* * * *

(8) "contents", when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication;

* * * *

(11) "aggrieved person" means a person who was a party to any intercepted wire, oral, or electronic communication or a person against whom the interception was directed;

* * * *

18 U.S.C. 2511

§ 2511. Interception and disclosure of wire, oral, or electronic communications prohibited

(1) Except as otherwise specifically provided in this chapter any person who--

(a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;

(b) * * * *

(c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;

(d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection; or

(e) * * * *

shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).

(2)(a) (i) It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

(ii) Notwithstanding any other law, providers of wire or electronic communication service, their officers, employees, and agents, landlords, custodians, or other persons, are authorized to provide information, facilities, or technical assistance to persons authorized by law to intercept wire, oral, or

electronic communications or to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, if such provider, its officers, employees, or agents, landlord, custodian, or other specified person, has been provided with--

(A) * * * *

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

setting forth the period of time during which the provision of the information, facilities, or technical assistance is authorized and specifying the information, facilities, or technical assistance required. No provider of wire or electronic communication service, officer, employee, or agent thereof, or landlord, custodian, or other specified person shall disclose the existence of any interception or surveillance or the device used to accomplish the interception or surveillance with respect to which the person has been furnished a court order or certification under this chapter, except as may otherwise be required by legal process and then only after prior notification to the Attorney General or to the principal prosecuting attorney of a State or any political subdivision of a State, as may be appropriate. Any such disclosure, shall render such person liable for the civil damages provided for in section 2520. No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, or agents, landlord, custodian, or other specified person for providing information, facilities, or assistance in accordance with the terms of a court order, statutory authorization, or certification under this chapter.

* * * *

(3)(a) Except as provided in paragraph (b) of this subsection, a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.

* * * *

* * * *

18 U.S.C. 2518

§ 2518. Procedure for interception of wire, oral, or electronic communications

* * * *

(7) Notwithstanding any other provision of this chapter, any investigative or law enforcement officer, specially designated by the Attorney General, the Deputy Attorney General, the Associate Attorney General, or by the principal prosecuting attorney of any State or subdivision thereof acting pursuant to a statute of that State, who reasonably determines that--

(a) an emergency situation exists that involves--

- (i) immediate danger of death or serious physical injury to any person,
- (ii) conspiratorial activities threatening the national security interest, or
- (iii) conspiratorial activities characteristic of organized crime,

that requires a wire, oral, or electronic communication to be intercepted before an order authorizing such interception can, with due diligence, be obtained, and

(b) there are grounds upon which an order could be entered under this chapter to authorize such interception,

may intercept such wire, oral, or electronic communication if an application for an order approving the interception is made in accordance with this section within forty-eight hours after the interception has occurred, or begins to occur. In the absence of an order, such interception shall immediately terminate when the communication sought is obtained or when the application for the order is denied, whichever is earlier. In the event such application for approval is denied, or in any other case where the interception is terminated without an order having been issued, the contents of any wire, oral, or electronic communication intercepted shall be treated as having been obtained in violation of this chapter, and an inventory shall be served as provided for in subsection (d) of this section on the person named in the application.

* * * *

18 U.S.C. 2520

§ 2520. Recovery of civil damages authorized

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

(b) Relief.--In an action under this section, appropriate relief includes--

- (1) such preliminary and other equitable or declaratory relief as may be appropriate;
- (2) damages under subsection (c) and punitive damages in appropriate cases; and
- (3) a reasonable attorney's fee and other litigation costs reasonably incurred.

(c) Computation of damages.--(1) * * * *

(2) In any other action under this section, the court may assess as damages whichever is the greater of--

- (A) the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation; or
- (B) statutory damages of whichever is the greater of \$100 a day for each day of violation or \$10,000.

* * * *

Stored Communication Act of 1986, as amended
18 U.S.C. 2701-2712

18 U.S.C. 2702

§ 2702. Voluntary disclosure of customer communications or records

(a) Prohibitions.--Except as provided in subsection (b) or (c)--

(1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and

(2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service--

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service;

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing; and

(3) a provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by paragraph (1) or (2)) to any governmental entity.

(b) Exceptions for disclosure of communications.--A provider described in subsection (a) may divulge the contents of a communication--

* * * *

(2) as otherwise authorized in section 2517, 2511(2)(a), or 2703 of this title;

* * * *

* * * *

18 U.S.C. 2703

§ 2703. Required disclosure of customer communications or records

* * * *

(e) No cause of action against a provider disclosing information under this chapter.--No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, subpoena, statutory authorization, or certification under this chapter.

* * * *

18 U.S.C. 2707

§ 2707. Civil action

(a) Cause of action.--Except as provided in section 2703(e), any provider of electronic communication service, subscriber, or other person aggrieved by any violation of this chapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action, recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate.

(b) Relief.--In a civil action under this section, appropriate relief includes--

- (1) such preliminary and other equitable or declaratory relief as may be appropriate;
- (2) damages under subsection (c); and
- (3) a reasonable attorney's fee and other litigation costs reasonably incurred.

(c) Damages.--The court may assess as damages in a civil action under this section the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation, but in no case shall a person entitled to recover receive less than the sum of \$1,000. If the violation is willful or intentional, the court may assess punitive damages. In the case of a successful action to enforce liability

under this section, the court may assess the costs of the action, together with reasonable attorney fees determined by the court.

* * * *

(e) Defense.--A good faith reliance on--

(1) * * * ;

(2) a request of an investigative or law enforcement officer under section 2518(7) of this title; or

(3) a good faith determination that section 2511(3) of this title permitted the conduct complained of;

is a complete defense to any civil or criminal action brought under this chapter or any other law.

* * * *

18 U.S.C. 2711

§ 2711. Definitions for chapter

As used in this chapter--

(1) the terms defined in section 2510 of this title have, respectively, the definitions given such terms in that section;

* * * *

(4) the term "governmental entity" means a department or agency of the United States or any State or political subdivision thereof.

Pen Register Act of 1986, as amended
18 U.S.C. 3121-3127

18 U.S.C. 3121

§ 3121. General prohibition on pen register and trap and trace device use; exception

(a) In general.--Except as provided in this section, no person may install or use a pen register or a trap and trace device without first obtaining a court order under section 3123 of this title or under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.).

* * * *

18 U.S.C. 3127

§ 3127. Definitions for chapter

As used in this chapter--

(1) the terms “wire communication”, “electronic communication”, “electronic communication service”, and “contents” have the meanings set forth for such terms in section 2510 of this title;

* * * *

(3) the term “pen register” means a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication, but such term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business;

(4) the term “trap and trace device” means a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication;

**Communications Act of 1934, Sections 222, 705, as amended
47 U.S.C. 222, 605**

47 U.S.C. 222

§ 222. Privacy of customer information

* * * *

(c) Confidentiality of customer proprietary network information

(1) Privacy requirements for telecommunications carriers

Except as required by law or with the approval of the customer, a telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service shall only use, disclose, or permit access to individually identifiable customer proprietary network information in its provision of (A) the telecommunications service from which such information is derived, or (B) services necessary to, or used in, the provision of such telecommunications service, including the publishing of directories.

* * * *

(h) Definitions

As used in this section:

(1) Customer proprietary network information

The term "customer proprietary network information" means--

(A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and

(B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier;

except that such term does not include subscriber list information.

* * * *

47 U.S.C. 605

§ 605. Unauthorized publication or use of communications

(a) Practices prohibited

Except as authorized by chapter 119, Title 18, no person receiving, assisting in receiving, transmitting, or assisting in transmitting, any interstate or foreign communication by wire or radio shall divulge or publish the existence, contents, substance, purport, effect, or meaning thereof, except through authorized channels of transmission or reception, (1) to any person other than the addressee, his agent, or attorney, (2) to a person employed or authorized to forward such communication to its destination, (3) to proper accounting or distributing officers of the various communicating centers over which the communication may be passed, (4) to the master of a ship under whom he is serving, (5) in response to a subpoena issued by a court of competent jurisdiction, or (6) on demand of other lawful authority. * * * *

* * * *

(d) Definitions

For purposes of this section--

* * * *

(6) the term "any person aggrieved" shall include any person with proprietary rights in the intercepted communication by wire or radio, including wholesale or retail distributors of satellite cable programming, and, in the case of a violation of paragraph (4) of subsection (e) of this section, shall also include any person engaged in the lawful manufacture, distribution, or sale of equipment necessary to authorize or receive satellite cable programming.

(e) Penalties; civil actions; remedies; attorney's fees and costs; computation of damages; regulation by State and local authorities

* * * *

(3)(A) Any person aggrieved by any violation of subsection (a) of this section or paragraph (4) of this subsection may bring a civil action in a United States district court or in any other court of competent jurisdiction.

(B) The court--

- (i) may grant temporary and final injunctions on such terms as it may deem reasonable to prevent or restrain violations of subsection (a) of this section;
- (ii) may award damages as described in subparagraph (C); and
- (iii) shall direct the recovery of full costs, including awarding reasonable attorneys' fees to an aggrieved party who prevails.

(C)(i) Damages awarded by any court under this section shall be computed, at the election of the aggrieved party, in accordance with either of the following subclauses;

(I) the party aggrieved may recover the actual damages suffered by him as a result of the violation and any profits of the violator that are attributable to the violation which are not taken into account in computing the actual damages; * * * or

(II) the party aggrieved may recover an award of statutory damages for each violation of subsection (a) of this section involved in the action in a sum of not less than \$1,000 or more than \$10,000, as the court considers just, * * * .

(ii) In any case in which the court finds that the violation was committed willfully and for purposes of direct or indirect commercial advantage or private financial gain, the court in its discretion may increase the award of damages, whether actual or statutory, by an amount of not more than \$100,000 for each violation of subsection (a) of this section.

(iii) In any case where the court finds that the violator was not aware and had no reason to believe that his acts constituted a violation of this section, the court in its discretion may reduce the award of damages to a sum of not less than \$250.

(4) Any person who manufactures, assembles, modifies, imports, exports, sells, or distributes any electronic, mechanical, or other device or equipment, knowing or having reason to know that the device or equipment is primarily of assistance in the unauthorized decryption of satellite cable programming, or direct-to-home satellite services, or is intended for any other activity prohibited by subsection (a) of this section, shall be fined not more than \$500,000 for each violation, or imprisoned for not more than 5 years for each violation, or both. For purposes of all penalties and remedies established for violations of this paragraph, the prohibited activity established herein as it applies to each such device shall be deemed a separate violation.

* * * *

CERTIFICATE OF COMPLIANCE

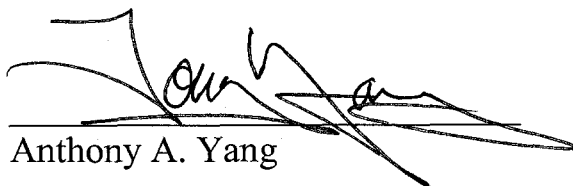
I hereby certify that this brief is in compliance with Rule 32(a)(7) of the Federal Rules of Appellate Procedure. The public and classified versions of this brief contain no more than 14,000 words, and were prepared in 14-point Times New Roman font using Corel WordPerfect 12.0.

CERTIFICATE OF SERVICE

I further certify that on this 9th day of March, 2007, I caused to be served via Federal Express two true and correct copies of the foregoing brief properly addressed to the following:

Robert D. Fram, Esq.
Michael M. Markman, Esq.
Heller Ehrman, LLP
333 Bush Street
San Francisco, CA 94104-2878
415-772-6000
Counsel for Plaintiffs-Appellees

Bradford A. Berenson, Esq.
David Lawson, Esq.
Edward R. McNicholas, Esq.
Sidley Austin, LLP
1501 K Street, NW
Washington, DC 20005
202-736-8010
Counsel for Defendants


Anthony A. Yang