

*In the*  
**United States Court of Appeals**  
*For the*  
**Ninth Circuit**

---

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

v.

AT&T CORP.,  
*Defendant-Appellant,*

UNITED STATES OF AMERICA,  
*Intervenor-Appellant.*

---

*Appeal from a decision of the United States District Court for the  
Northern District of California (San Francisco), No. 06-CV-00672 · Honorable Vaughn R. Walker*

---

---

**CORRECTED ANSWERING BRIEF OF PLAINTIFFS-APPELLEES  
SEALED**

---

---

ELECTRONIC FRONTIER FOUNDATION  
CINDY COHN, ESQ.  
LEE TIEN, ESQ.  
KURT OPSAHL, ESQ.  
KEVIN S. BANKSTON, ESQ.  
JAMES S. TYRE, ESQ.  
454 Shotwell Street  
San Francisco, California 94110  
(415) 436-9333 Telephone  
(415) 436-9993 Facsimile

HELLER EHRMAN LLP  
ROBERT D. FRAM, ESQ.  
E. JOSHUA ROSENKRANZ, ESQ.  
MICHAEL M. MARKMAN, ESQ.  
ETHAN C. GLASS, ESQ.  
SAMUEL F. ERNST, ESQ.  
NATHAN E. SHAFROTH, ESQ.  
ELENA M. DIMUZIO, ESQ.  
333 Bush Street  
San Francisco, California 94104  
(415) 772-6000 Telephone  
(415) 772-6268 Facsimile

*Attorneys for Appellees Tash Hepting, et al.*

***Additional Counsel Listed Inside Cover***



LAW OFFICE OF RICHARD R. WIEBE  
RICHARD R. WIEBE, ESQ.  
425 California Street, Suite 2025  
San Francisco, California 94104  
(415) 433-3200 Telephone  
(415) 433-6382 Facsimile

HAGENS BERMAN SOBEL SHAPIRO LLP  
REED R. KATHREIN, ESQ.  
JEFFREY FRIEDMAN, ESQ.  
SHANA E. SCARLETT, ESQ.  
425 Second Street, Suite 500  
San Francisco, California 94107  
(415) 896-6300 Telephone  
(415) 896-6301 Facsimile

LERACH COUGHLIN STOIA  
GELLER RUDMAN & ROBBINS LLP  
ERIC A. ISAACSON, ESQ.  
655 West Broadway, Suite 1900  
San Diego, California 92101-3301  
(619) 231-1058 Telephone  
(619) 231-7423 Facsimile

LAW OFFICE OF ARAM ANTARAMIAN  
ARAM ANTARAMIAN, ESQ.  
1714 Blake Street  
Berkeley, California 94703  
(510) 841-2369 Telephone

*Attorneys for Appellees Tash Hepting, et al.*

## TABLE OF CONTENTS

	<u>Page</u>
TABLE OF AUTHORITIES .....	iv
INTRODUCTION .....	1
QUESTIONS PRESENTED .....	4
STATEMENT OF FACTS .....	5
An AT&T Employee Details AT&T’s Collaboration in Dragnet Surveillance .....	5
AT&T Intercepts Communications in Other Cities .....	9
The Government Publicly Confirms that it Conducted Warrantless Surveillance Without Complying With FISA and Members of Congress and Telecommunications Carriers Confirm Dragnet Surveillance.....	10
Plaintiffs File this Suit .....	14
The Government Intervenes to Seek Dismissal, But Concedes that Plaintiffs’ Evidence Is Not Privileged .....	15
The Government Submits the “Terrorist Surveillance Program” for FISA Review .....	16
SUMMARY OF ARGUMENT .....	17
ARGUMENT.....	19
I.    THE STATE SECRETS PRIVILEGE IS A NARROW, EVIDENTIARY PRIVILEGE AND IS NOT AN IMMUNITY FROM SUIT.....	19
II.   THE DISTRICT COURT CORRECTLY CONCLUDED THAT THE VERY SUBJECT MATTER OF THIS SUIT IS NOT A STATE SECRET.....	24
A.   Congress Has Determined that the Very Subject Matter of this Case Is Not a State Secret that Warrants Dismissal. ....	25
1.   Congress has directed the procedure for assessing claims of national security in electronic surveillance cases, and does not allow dismissal on the pleadings. ....	26

**TABLE OF CONTENTS**

	<b><u>Page</u></b>
2. Congress struck that balance because it did not want the Executive to shield illegal surveillance with sweeping assertions of national security.....	31
3. FISA’s procedure for handling state secrets applies to this case. ....	33
B. The Very Subject Matter of this Suit Is Not a Secret.....	36
1. The evidence already submitted establishes that AT&T collaborated with the NSA in electronic surveillance, and the Government has conceded that the evidence is not a state secret.....	37
2. The Government’s concession was correct. ....	39
3. Public statements by Government officials and others confirm that disclosure of communications records to the Government is not a secret. ....	43
C. This Case Is Distinguishable from Decisions in which the Entire Subject Matter of the Action Was a State Secret and Where the Case Was Dismissed After Discovery.....	45
1. This case is not subject to the <i>Totten</i> bar. ....	46
2. The handful of other opinions dismissing cases at the inception are also distinguishable.....	49
3. Cases applying the state secrets privilege to specific discovery issues do not support dismissal on the pleadings.....	52
D. No Common Law Doctrine Could Override The Court’s Responsibility to Consider a Case of Massive Dragnet Surveillance. ....	55
III. LOOKING BEYOND THIS APPEAL, LITIGATING THIS CASE AS CONGRESS INTENDED WILL NOT REQUIRE DISCOVERY OF STATE SECRETS, GIVEN THE LIMITED NATURE OF THE EVIDENCE NECESSARY TO PROVE PLAINTIFFS’ CLAIMS AND THE LIMITED NATURE OF AT&T’S POSSIBLE DEFENSES. ....	58

**TABLE OF CONTENTS**

	<b><u>Page</u></b>
A.    Plaintiffs Will Be Able To Prove Their Claims .....	60
B.    AT&T Will Have a Fair Opportunity to Defend Itself.....	64
IV.    THE DISTRICT COURT CORRECTLY DENIED THE MOTIONS TO DISMISS THE COMPLAINT ON STANDING GROUNDS.....	68
A.    Plaintiffs’ Allegations Defeat a Motion to Dismiss at the Pleading Stage. ....	69
B.    Plaintiffs Are Not Required to <i>Prove</i> Standing at this Early Stage.....	72
C.    The Evidence Plaintiffs Have Already Adduced Is Sufficient to Satisfy Standing. ....	75
1.    The evidence already adduced establishes that AT&T diverts all, or substantially all, of the peered internet traffic in the area.....	75
2.    The evidence establishes standing both to sue over past interceptions and to enjoin future ones.....	76
D.    Any Further Evidence Plaintiffs Might Need to Establish Standing Can Be Gathered Without Divulging State Secrets.....	80
E.    The Decisions AT&T Invokes Do Not Justify Dismissal of a Dragnet Case Involving Dragnet Surveillance on the Pleadings. ....	82
CONCLUSION .....	86
Appendix: Plaintiffs Can Support Each Element Of Their Statutory Claims With Non-Privileged Evidence .....	88
CERTIFICATE OF COMPLIANCE.....	91
STATEMENT OF RELATED CASES.....	92
ADDENDUM	
DECLARATION OF SERVICE	

## TABLE OF AUTHORITIES

Page

### Cases

<i>ACLU Foundation of Southern Cal. v. Barr</i> , 952 F.2d 457 (D.C. Cir. 1991) .....	33, 34
<i>ACLU v. NSA</i> , 438 F. Supp. 2d 754 (E.D. Mich. 2006) .....	63
<i>American Library Ass 'n v. FCC</i> , 401 F.3d 489 (D.C. Cir. 2005) .....	78
<i>Andresen v. Maryland</i> , 427 U.S. 463 (1976).....	63
<i>Bareford v. General Dynamics Corp.</i> , 973 F.2d 1138 (5th Cir. 1992).....	40, 41
<i>Baur v. Veneman</i> , 352 F.3d 625 (2d Cir. 2003).....	78, 79
<i>Berger v. New York</i> , 388 U.S. 41 (1967).....	55, 56
<i>Bourjaily v. United States</i> , 483 U.S. 171 (1987).....	44
<i>Bowles v. United States</i> , 950 F.2d 154 (4th Cir. 1991).....	21
<i>Camara v. Municipal Ct.</i> , 387 U.S. 523 (1967).....	57
<i>Capital Cities Media, Inc. v. Toole</i> , 463 U.S. 1303 (1983).....	36
<i>Central Delta Water Agency v. United States</i> , 306 F.3d 938 (9th Cir. 2002).....	74, 79
<i>Clift v. United States</i> , 597 F.2d 826 (2d Cir. 1979).....	22, 23

## TABLE OF AUTHORITIES

	<u>Page</u>
<i>Clinton v. New York</i> , 524 U.S. 417 (1998).....	78, 79
<i>Connecticut Gen. Life Ins. Co. v. New Images of Beverly Hills</i> , 321 F.3d 878 (9th Cir. 2003).....	64
<i>Covington v. Jefferson County</i> , 358 F.3d 626 (9th Cir. 2004).....	78
<i>Crater Corp. v. Lucent Techs., Inc.</i> , 423 F.3d 1260 (Fed. Cir. 2005).....	23
<i>DTM Research L.L.C. v. AT&amp;T Corp.</i> , 245 F.3d 327 (4th Cir. 2001).....	21
<i>Edmond v. United States</i> , 520 U.S. 651 (1997).....	35
<i>Ellsberg v. Mitchell</i> , 709 F.2d 51 (D.C. Cir. 1983) .....	<i>passim</i>
<i>El-Masri v. United States</i> , 479 F.3d 296 (4th Cir. 2007).....	50, 51
<i>Entick v. Carrington</i> , 19 How. St. Tr. 1029 (1765) .....	55
<i>Ex Parte Milligan</i> , 71 U.S. 2 (1866).....	57
<i>FEC v. Akins</i> , 524 U.S. 11, 24 (1998).....	71
<i>Fitzgerald v. Penthouse Int’l, Ltd.</i> , 776 F.2d 1236 (4th Cir. 1985).....	22, 54
<i>Friends of the Earth, Inc. v. Gaston Copper Recycling Corp.</i> , 204 F.3d 149 (4th Cir. 2000).....	79
<i>Go-Bart Importing Co. v. United States</i> , 282 U.S. 344 (1931).....	63

## TABLE OF AUTHORITIES

	<u>Page</u>
<i>Halkin v. Helms</i> , 598 F.2d 1 (D.C. Cir. 1978) .....	<i>passim</i>
<i>Halkin v. Helms</i> , 690 F.2d 977 (D.C. Cir. 1982) .....	<i>passim</i>
<i>Hall v. Norton</i> , 266 F.3d 969 (9th Cir. 2001).....	78
<i>Hamdan v. Rumsfeld</i> , 126 S.Ct. 2749 (2006).....	57
<i>Hamdi v. Rumsfeld</i> , 542 U.S. 507 (2004).....	57
<i>Heine v. Raus</i> , 399 F.2d 785 (4th Cir. 1968).....	21
<i>Helling v. McKinney</i> , 509 U.S. 25 (1993).....	78, 79
<i>Hepting v. AT&amp;T Corp.</i> , 439 F. Supp. 2d 974 (N.D. Cal. 2006).....	<i>passim</i>
<i>In re State Police Litigation</i> , 888 F. Supp. 1235 (D. Conn. 1995) .....	61
<i>In re Under Seal</i> , 945 F.2d 1285 (4th Cir. 1991).....	21
<i>In re United States</i> , 872 F.2d 472 (D.C. Cir. 1989) .....	21, 22, 23
<i>Kasza v. Browner</i> , 133 F.3d 1159 (9th Cir. 1998).....	<i>passim</i>
<i>LaDuke v. Nelson</i> , 762 F.2d 1318 (9th Cir. 1985).....	79, 80
<i>Linder v. Nat'l Sec. Agency</i> , 94 F.3d 693 (D.C. Cir. 1996) .....	21

## TABLE OF AUTHORITIES

	<u>Page</u>
<i>Lujan v. Defenders of Wildlife</i> , 504 U.S. 555 (1992).....	68, 72
<i>Marcus v. Search Warrant of Prop.</i> , 367 U.S. 717 (1961).....	63
<i>McGehee v. Casey</i> , 718 F.2d 1137 (D.C. Cir. 1983) .....	36
<i>Molerio v. FBI</i> , 749 F.2d 815 (D.C. Cir. 1984) .....	21, 24
<i>Monarch Assurance P.L.C. v. United States</i> , 244 F.3d 1356 (Fed. Cir. 2001) .....	23
<i>National Coal. for Students with Disabilities Educ. and Legal Defense Fund v. Scales</i> , 150 F. Supp. 2d 845 (D. Md. 2001).....	73
<i>Northrop Corp. v. McDonnell Douglas Corp.</i> , 751 F.2d 395 (D.C. Cir. 1984) .....	21
<i>Spock v. United States</i> , 464 F. Supp. 510 (S.D.N.Y. 1978) .....	43
<i>Stanford v. Texas</i> , 379 U.S. 476 (1965).....	63
<i>States v. Belfield</i> , 692 F.2d 141 (D.C. Cir. 1982) .....	31
<i>Steel Co. v. Citizens for a Better Env't</i> , 523 U.S. 83 (1998).....	73
<i>Sterling v. Tenet</i> , 416 F.3d 338 (4th Cir. 2005).....	50, 51
<i>Tenet v. Doe</i> , 544 U.S. 1 (2005).....	24, 46, 47, 48
<i>Totten v. United States</i> , 92 U.S. 105 (1875).....	<i>passim</i>

## TABLE OF AUTHORITIES

	<u>Page</u>
<i>United States v. Belfield</i> , 692 F.2d 141 (D.C. Cir. 1982) .....	31
<i>United States v. Calandra</i> , 414 U.S. 338 (1974).....	56
<i>United States v. Ott</i> , 827 F.2d 473 (9th Cir. 1987).....	33
<i>United States v. Pawlinski</i> , 374 F.3d 536 (7th Cir. 2004).....	79
<i>United States v. Reynolds</i> , 345 U.S. 1 (1953).....	<i>passim</i>
<i>United States v. Stanley</i> , 483 U.S. 669 (1987).....	59
<i>Webster v. Doe</i> , 486 U.S. 592 (1988).....	56
<i>Weil v. Invest./Indicators, Research &amp; Mgmt.</i> , 647 F.2d 18 (9th Cir. 1981).....	66
<i>Weinberger v. Catholic Action of Hawaii/Peace Education Project</i> , 454 U.S. 139 (1981).....	48, 49
<i>Yamaha Motor Corp. v. Calhoun</i> , 516 U.S. 199 (1996).....	59
<i>Youngstown Sheet &amp; Tube Co. v. Sawyer</i> , 343 U.S. 579 (1952).....	33, 57
<i>Zuckerbraun v. Gen. Dynamics Corp.</i> , 935 F.2d 544 (2d Cir. 1991).....	51
 <b>Statutes</b>	
18 U.S.C. § 2510(4) .....	61, 88
18 U.S.C. § 2510(5) .....	88

## TABLE OF AUTHORITIES

	<u>Page</u>
18 U.S.C. § 2510(8).....	35
18 U.S.C. § 2511.....	88
18 U.S.C. § 2511(1)(a).....	60
18 U.S.C. § 2511(1)(c).....	60, 89
18 U.S.C. § 2511(2)(a)(ii).....	66, 67
18 U.S.C. § 2511(2)(f).....	26
18 U.S.C. § 2511(3)(a).....	60, 89
18 U.S.C. § 2520(a).....	26
18 U.S.C. § 2702(a)(3).....	61, 89
18 U.S.C. § 2707(a).....	26
47 U.S.C. § 605(e)(3)(A).....	26
50 U.S.C. § 1801(f).....	88
50 U.S.C. § 1801(f)(2).....	35, 61
50 U.S.C. § 1801(k).....	33
50 U.S.C. § 1801(n).....	35
50 U.S.C. § 1806(f).....	<i>passim</i>
50 U.S.C. § 1809.....	26
50 U.S.C. § 1809(a).....	26, 60, 88
50 U.S.C. § 1810.....	26
50 U.S.C. § 402 note.....	35
50 U.S.C. § 403-1(i)(1).....	35

## TABLE OF AUTHORITIES

Page

### **Other Authorities**

Exec. Order § 12968 §§ 1.2(a), 1.1(h), 1.1(e).....	88, 89
H.R. Conf. Rep. No. 95-1720 (1978) .....	30, 33
S. Rep. No. 95-604(I) (1978) .....	<i>passim</i>
S. Rep. No. 95-701 (1978) .....	30
S. Rep. No. 94-755 (1976) .....	<i>passim</i>
Wright & Graham, 26 Fed. Prac. & Proc. § 5665 .....	42

### **Rules**

Federal Rule App. Proceedings 32(a)(7)(B)(iii) .....	91
Federal Rule of Civil Proceedings 56(f).....	73
Federal Rule of Evidence 104(a).....	44
Federal Rule of Evidence 501 .....	65

## **INTRODUCTION**

Plaintiffs are challenging the most extensive surveillance dragnet in American history: AT&T indiscriminately intercepted and disclosed to the Government the telephone and internet communications of millions of customers, along with detailed records about customers' communications.

This allegation is based on detailed and unrebutted evidence. A former AT&T employee has sworn to his personal observations and has presented over a hundred pages of authenticated AT&T schematic diagrams and tables detailing how AT&T diverted communications to the National Security Agency ("NSA"). No fewer than 19 members of Congress have publicly confirmed, based upon briefings from the Executive Branch, that telecommunications companies turned over to the Government huge databases of information about telephone and other communications. And carriers, themselves, have confirmed that the Government approached them to assist in these surveillance efforts.

The central claim in this case is that the dragnet flouted Congress's specific regulatory scheme, most notably, the Foreign Intelligence Surveillance Act ("FISA"), invading the privacy rights of AT&T customers. These statutes are categorical: If AT&T participated in a Government surveillance program and the program bypassed Congress's requirements, AT&T is liable. Period. To prove their case, Plaintiffs need not demonstrate, much less discover, why the NSA asked

AT&T to intercept and disclose its customers' communications and records, which communications from the dragnet drew the NSA's attention, or what the NSA did with the information it gleaned from the dragnet. Nor would such details afford AT&T any defense.

Nevertheless, the Government has intervened in this case, invoking the state secrets privilege. It insists that the very existence of this case poses a "grievous" threat to national security. Gov. 11.<sup>1</sup> The Government seeks an extraordinary remedy—dismissal at the outset of the case—that is almost never granted, even in foreign intelligence cases. In an effort to meet the forbidding standards set out in this Court's precedents, the Government contends that the basic question of whether AT&T collaborated in the dragnet is a state secret that Plaintiffs should never be allowed to prove. According to the Government, the Executive and its telecommunications collaborators are free to eavesdrop on every American with impunity. They can do so without a warrant, without suspicion, and without accountability in any court. Once the Government invokes the shibboleth of national security, the case is over.

---

<sup>1</sup> Throughout this brief, "AER" refers to the excerpts of record submitted by Defendant AT&T Corp. "GER" refers to the excerpts of record submitted by the United States. "SER" refers to the Supplemental Excerpts of Record submitted by Plaintiffs. The Government's brief and AT&T's brief are cited as "Gov." and "AT&T," respectively. Amicus briefs are cited by the name or abbreviation of the lead amicus, as follows: "\_\_\_ Br."

Congress has directed otherwise. When Congress created a cause of action directed at wiretapping in the name of “Foreign Intelligence Surveillance,” it knew that many—perhaps all—of the ensuing cases would involve claimed state secrets. In reaction to “revelations that warrantless electronic surveillance in the name of national security has been seriously abused,” Congress struck a balance. S. Rep. No. 95-604(I), 7 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3904, 3908. It created a five-step protocol to be followed whenever the Government contends that certain information relating to electronic surveillance would implicate national security concerns. *See* 50 U.S.C. § 1806(f). The protocol does not permit dismissal at the inception of an electronic surveillance case just because the Government contends the case involves state secrets.

So much is true even for the garden-variety electronic surveillance claim. Here dismissal on the basis of state secrets is especially inappropriate, because the Government itself has made a carefully considered judgment that the unrebutted record evidence establishing AT&T’s participation in the Government’s dragnet electronic surveillance program is not covered by the state secrets privilege. The Assistant Attorney General was emphatic about the point: “None of the documents [Plaintiffs] have submitted to accompany these declarations implicate any privileged matters. . . . We have not asserted a privilege over either [the declarations or their exhibits].” AER 189.

This carefully considered decision not to assert any privilege over Plaintiffs' evidence means that the very subject matter of this suit cannot be a state secret. And even without the Government's concession, the long and growing list of public admissions about massive disclosures of the details of communications means that it is simply no longer a secret that AT&T assisted the NSA in its illegal surveillance program.

If, as the case unfolds, Plaintiffs seek particular evidence that is a state secret, the Government will have every opportunity to demonstrate that the specific information sought is too sensitive to be revealed. But for now, the District Court's order denying the Government's motion to dismiss must be affirmed.

### **QUESTIONS PRESENTED**

1. Congress has decided that a case challenging electronic surveillance must not be dismissed at the outset, and in this case, AT&T's participation in electronic surveillance is no secret. Was the District Court correct in denying the extraordinary remedy of dismissal on state secrets grounds?

2. Have Plaintiffs alleged sufficient facts to establish standing at the pleadings stage, where they have alleged that their communications and communications records have been unlawfully intercepted and disclosed?

## STATEMENT OF FACTS

### *An AT&T Employee Details AT&T's Collaboration in Dragnet Surveillance*

This case began when a former AT&T employee named Mark Klein came forward with detailed eyewitness testimony and documentary evidence proving that AT&T has been collaborating with the NSA in the surveillance of the domestic communications of millions of Americans. Mr. Klein had worked as an AT&T technician for 22 years, most recently at AT&T's San Francisco facility. He described events and operations he had observed at AT&T in a sworn declaration laden with self-verifying detail. SER 1-136.

Mr. Klein's account begins around January 2003, when the manager of his facility advised him that the NSA was coming to interview another colleague for a "special job." SER 3. The "special job" was to install equipment in a high-security room AT&T was building at its Folsom Street Facility in San Francisco. *Id.* The NSA supervised the construction and outfitting of the room, which came to be known as the "SG3 Secure Room." *Id.* Mr. Klein personally saw the room when it was under construction, and, at one point, entered the room briefly after it was fully operational. SER 3-4.

In October 2003, AT&T transferred Mr. Klein to the Folsom Street Facility. SER 3. Although AT&T entrusted Mr. Klein with keys to every other door at the Folsom Street Facility, he did not have access to the SG3 Secure Room. SER 4.

No AT&T employee was allowed in the secret room without NSA security clearance. *Id.*

Mr. Klein recounts one event that underscores the “extremely limited access to the SG3 Secure Room”: A large industrial air conditioner in the room began “leaking water through the floor and onto . . . equipment downstairs.” *Id.* AT&T maintenance personnel were not allowed to enter to fix the leak—or even to triage and prevent water damage to other portions of the facility. *Id.* Despite the “semi-emergency,” AT&T waited days for a repairman with NSA clearance to provide service. *Id.*

At the Folsom Street Facility, Mr. Klein’s job was to oversee AT&T’s “WorldNet Internet room.” SER 3. Communications carried by AT&T’s WorldNet Internet service pass through that room to be directed to or from customers. SER 4. The Folsom Street Facility also handles millions of telephone communications. SER 3.

Mr. Klein revealed that AT&T intercepts every single one of the communications passing through the WorldNet Internet room and directs them all to the NSA. SER 5-6. As Mr. Klein explained, the communications are carried as light signals on fiber-optic cables. SER 5. To divert the communications, AT&T connected the fiber-optic cables entering the WorldNet Internet room to a “splitter cabinet.” *Id.* The splitter cabinet splits the light signals from the WorldNet

Internet service in two, making two identical copies of the material carried on the light signal. *Id.* The splitter cabinet directed one portion of the light signal through fiber optic cables into the NSA's secret room while allowing the other portion to travel its normal course to its intended destination. SER 5-6. The split cables carried domestic and international communications of AT&T customers, as well as communications from users of other non-AT&T networks that pass through the Folsom Street Facility. SER 6.

Mr. Klein attached to his declaration two AT&T documents called "SIMS Splitter Cut-In and Test Procedure," which describe "how to connect the already in-service circuits to a 'splitter cabinet,' which diverted light signals from the WorldNet Internet service's fiber optical circuits to the SG3 Secure Room." SER 5, 9-75. He also attached a third AT&T document "describ[ing] the connections from the SG3 Secure Room on the 6th floor to the WorldNet Internet room on the 7th floor, and provid[ing] diagrams on how the light signal was being split." SER 6, 76-134. This document also "listed the equipment installed in the SG3 Secure Room." SER 6. These three documents comprise over 100 pages of highly technical details on the interceptions, including 57 detailed schematics and 24 tables of data.

James Russell, AT&T's Managing Director-Asset Protection, has confirmed that Mr. Klein's declaration and the AT&T documents Mr. Klein attached

accurately describe AT&T's internet network, AT&T's San Francisco communications facility and the location of specific equipment within the San Francisco facility, and the interconnection points of AT&T's internet network with the networks of other communications carriers. SER 508-09, 511-14. Mr. Russell confirmed the conclusion that the exhibits to the Klein Declaration are authentic AT&T documents that provide "detailed schematics of network wiring configurations that are uniform across AT&T locations and that are used by AT&T to cross-connect and split fiber cables" and "identif[y] the manufacturer and name of many pieces of equipment used by AT&T." SER 514.

Plaintiffs retained an expert in information technology and telecommunications to explain the implications of the documents and testimony Mr. Klein furnished. SER 137-506. The expert, J. Scott Marcus, spent decades working for a variety of telecommunications clients, including AT&T. He confirmed "Mr. Klein's allegation that the room described was a secure facility, intended to be used for purposes of surveillance on a very substantial scale." SER 142. He "conclude[d] that AT&T has constructed an extensive—and expensive—collection of infrastructure that collectively has all the capability necessary to conduct large scale covert gathering of IP-based communications information, *not only for communications to overseas locations, but for purely domestic*

*communications as well.*” SER 148 (emphasis in original). “This deployment,” he opines, “*is neither modest nor limited.*” SER 150 (emphasis in original).

The expert further concluded that “all or substantially all” of AT&T’s “peered traffic” in San Francisco was sent into the SG3 Secure Room, SER 165, meaning any communication between AT&T customers and non-AT&T customers. SER 162-65. AT&T made no effort to filter out purely domestic-to-domestic electronic communications, as a fiber splitter is not a selective device; all traffic on the split circuit was diverted or copied. SER 165-67.

#### ***AT&T Intercepts Communications in Other Cities***

That was just in San Francisco. From the arrangement of the hardware, Mr. Marcus concluded that AT&T’s surveillance “apparently involves considerably more locations than would be required to catch the majority of international traffic.” SER 7. Further evidence confirms the expert’s view. Mr. Klein reports “that other such ‘splitter cabinets’ were being installed in other cities, including Seattle, San Jose, Los Angeles and San Diego.” SER 7. Two former AT&T employees have revealed a similar secure room at an AT&T command center in St. Louis. SER 813-17. They report that “AT&T has maintained a secret, highly secured room since 2002 where government work is being conducted” and that “only government officials or AT&T employees with top-secret security clearance are admitted to the room.” SER 813.

According to Mr. Marcus, this web of surveillance facilities would probably capture well over half of AT&T's purely domestic traffic, representing almost all of the AT&T traffic to and from other providers. SER 169-70. This comprises about "10% of all purely domestic Internet communications in the United States," including non-AT&T customers. AER 106 (emphasis in original).

***The Government Publicly Confirms that it Conducted Warrantless Surveillance Without Complying With FISA and Members of Congress and Telecommunications Carriers Confirm Dragnet Surveillance***

On December 16, 2005, the *New York Times* broke the news that, for at least four years, the President had secretly authorized the NSA to intercept Americans' communications without warrants from the Foreign Intelligence Surveillance Court as required by the FISA. AER 36-41. The next day, President Bush admitted during a nationwide radio address that he had indeed authorized surveillance, but he described a limited program; he insisted the Government was targeting only international communications where one participant is suspected of being an al Qaeda associate. AER 43-44. The Government has been referring to this targeted aspect of its surveillance as the "Terrorist Surveillance Program," or "TSP." See Gov. 10-11.

About a week later, the *New York Times* published another story, reporting that anonymous officials had disclosed that the NSA's surveillance program was much broader than the targeted TSP President Bush had described. SER 610-12.

Consistent with the evidence from Mr. Klein, the article described how the NSA, with the cooperation of American telecommunications companies, analyzed large volumes of telephone and Internet communications acquired via “backdoor” access to major telecommunications switches inside the United States. *Id.*

The next day, the *Los Angeles Times* revealed that AT&T had similarly provided the NSA with a “direct hookup” to “Daytona,” its database of detailed communications records, records of who called whom, and the time and duration of the calls. GER 11; SER 613-15. In the ensuing months, *USA Today* further reported that AT&T not only assisted the NSA in intercepting the content of communications, SER 607-08, but also disclosed to the NSA tens of millions of communications records. SER 731-35.

Well over a dozen members of Congress who had been briefed by the Executive and two telecommunications carriers that had been approached by the Executive confirmed the disclosure of communications records to the NSA. The confirmations are so numerous and so similar that they can only be viewed as a coordinated effort to acknowledge—and defend—the surveillance. *See, e.g.*, SER 754 (19 members of congressional intelligence committees “verified that the NSA has built a database that includes records of Americans’ domestic phone calls”). For example, Sen. Christopher Bond publicly confirmed that “[t]he president’s program uses information collected from phone companies. . . . what telephone

number called what other telephone number.” SER 746. Then-Senate Majority Leader Bill Frist, too, confirmed that the NSA was collecting call records of tens of millions of Americans using data provided by AT&T. SER 720. When asked, “Are you comfortable with this program?” Sen. Frist replied, “Absolutely. Absolutely. I am one of the people who are briefed. . . . I’ve known about the program.” *Id.* Similarly, Sen. Saxby Chambliss confirmed that he had been briefed on the Government’s efforts to compile a database of the details of all telephone calls. SER 755. He bemoaned the fact that only some companies agreed to hand over the records: “It’s difficult to say you’re covering all terrorist activity in the United States if you don’t have all the (phone) numbers. . . . [I]t probably would be better to have records of every telephone company.” SER 755.

Sen. Pat Roberts, then-chair of the Senate Intelligence Committee, also confirmed that he had been briefed about the NSA’s success in collecting millions of phone records for domestic calls. He defended the program:

[W]ell, basically, if you want to get into that, we’re talking about business records. We’re not, you know, we’re not listening to anybody. This isn’t a situation where if I call you, you call me, or if I call home or whatever, that that conversation is being listened to.

SER 824.

Carriers have also admitted the existence and magnitude of the Government’s efforts to collect communications records. As the District Court recounted, Qwest Communications International Inc. publicly announced that

“Qwest was approached to permit the Government access to the private telephone records of Qwest customers.” 439 F. Supp. 2d at 988. When Qwest learned that no legal process had been secured in support of the request and that “there was a disinclination on the part of the authorities to use any legal process, including the Special Court which had been established to handle such matters,” Qwest “declined to participate in the program.” *Id.* These requests continued until at least June of 2002.

The Government appears to have made no effort to staunch the flow of public information about the existence of these programs. Even while this appeal was pending members of Congress and carriers continued to make these sorts of revelations. Verizon Wireless confirmed that the Government sought “billions of private phone records” from that company. SER 844.<sup>2</sup> A Verizon spokesperson admitted: “Absolutely, absolutely. We were asked, but we said, no, we would not give that information, again, you know, trying to protect the privacy of our customers. We take that very seriously.” *Id.* See also SER 832 (Rep. Jane Harman acknowledges “a program that involves the collection of some phone records”).

---

<sup>2</sup> While these revelations are obviously not part of the record on appeal, we recount them simply to support the District Court’s expectation that more facts about AT&T’s disclosure of communications records would materialize. *Hepting v. AT&T Corp.*, 439 F. Supp. 2d 974, 997-98 (N.D. Cal. 2006).

### ***Plaintiffs File this Suit***

On January 31, 2006, Plaintiffs filed this lawsuit against AT&T as a class action on behalf of AT&T's residential customers. Plaintiffs specifically alleged that AT&T has been and continues to intercept and disclose their internet and telephone communications, as well as their communications records, *en masse*, to the Government without legal process or authority.

The First Amended Complaint alleges violations of several statutory and constitutional rights. At the heart of the case lie four interrelated federal statutes. The first is FISA. GER 19-20. The second is Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended by the Electronic Communications Privacy Act of 1986 ("ECPA"). GER 21-22. The third is the Stored Communications Act ("SCA") portion of the ECPA. GER 24-26. The fourth is the Communications Act of 1934. GER 23-24. Together, these statutes comprise a comprehensive legislative scheme governing electronic surveillance. As a general matter, these statutes prohibit AT&T from intercepting any electronic communications and from disclosing any intercepted communications or communication records—except pursuant to strict statutory procedures.

Plaintiffs further allege that AT&T has violated the First and Fourth Amendments to the United States Constitution by acting as Government agents in illegally intercepting and disclosing Plaintiffs' communications and

communications records. GER 17-19. Plaintiffs also allege that AT&T violated California's Unfair Competition Law. GER 26-29.

Plaintiffs seek injunctive relief, declaratory relief, and damages. GER 29-31.

***The Government Intervenes to Seek Dismissal, But Concedes that Plaintiffs' Evidence Is Not Privileged***

With the case in its infancy, before AT&T answered the complaint and before Plaintiffs obtained any discovery, the Government moved to intervene as a defendant and moved to dismiss based on an assertion of the state secrets privilege. It alternatively sought summary judgment on the same grounds. The Government claimed that the very existence of this lawsuit threatens national security. SER 659-60. AT&T also moved to dismiss on the ground that Plaintiffs had not alleged sufficient facts to establish standing. SER 628.

The Government, for its part, made a considered judgment from the outset of this case to narrow the scope of its state secrets argument: Not only did the Government decline to object to the admission of the Klein and Marcus declarations and AT&T documents, but it affirmatively declared that these documents are not subject to the state secrets privilege. The Government deliberately emphasized that it was not trying to suppress evidence that was already in the public arena. Toward that end, the Assistant Attorney General began his oral argument on the motion with the declaration that, "We don't want to

unring that bell.” AER 189. “*We have not asserted any privilege over the information that is in the Klein and Marcus declarations.*” AER 189 (emphasis added). At the District Court’s prompting the Government’s lead lawyer clarified that “[w]e have not asserted a privilege over either [the declaration or their exhibits].” *Id.* (emphasis added). The declarations at the heart of this case remain partially sealed only because *AT&T* has claimed they are trade secrets. *See* SER 509.

The District Court denied both *AT&T*’s and the Government’s motions to dismiss. *Hepting*, 439 F. Supp. 2d at 974.

### ***The Government Submits the “Terrorist Surveillance Program” for FISA Review***

On January 17, 2007, while this appeal was pending, the Government executed an abrupt about-face. The Attorney General wrote a letter to the Senate Judiciary Committee confirming that the Executive had not been adhering to FISA’s strictures, and declaring that the Executive is now seeking periodic FISA Court approval for the targeted Terrorist Surveillance Program that the President had publicly acknowledged. GER 341. The Government has coyly declined to say anything about whether it has subjected its dragnet surveillance—capturing massive numbers of communications and related data—to any judicial scrutiny. The omission is especially telling because the Government insists here that the targeted program is distinct from the dragnets. *See* Gov. 3, 9-10.

## SUMMARY OF ARGUMENT

The Government invokes the state secrets privilege to block Plaintiffs' case at the threshold, before the complaint has been answered and before discovery has begun. This Court has held that the common law evidentiary privilege allows such a draconian result only in one rare circumstance: where the very subject matter of the suit is a state secret, and even then only where Congress has not superseded the common law privilege by statute. Otherwise, any invocation of the privilege must await specific evidentiary or discovery disputes—if ever they arise.

The subject matter of this suit is straightforward: Whether AT&T participated in an illegal dragnet surveillance program. The core secret the Government purports to protect is the basic question “[w]hether AT&T is involved in either the TSP or the broader activities alleged by plaintiffs.” Gov. 10. That subject matter cannot be a state secret for two main reasons.

*First*, Congress has made a different choice. In enacting FISA, it determined that a telephone company's participation in electronic surveillance at the behest of the Government is subject to private rights of action. Congress knew that such lawsuits would typically involve state secrets; that is what “Foreign Intelligence Surveillance” means. Yet Congress declared that in any case involving the legality of foreign intelligence electronic surveillance there is the potential that *some* secret information may well have to be turned over, subject to appropriate protective

precautions. This necessarily means that the Executive must be wrong when it claims *ex ante* that the entire subject matter of an electronic surveillance case is a state secret. Congress also dictated a protocol that the courts must follow where the Government invokes the privilege. This protocol never entails dismissal at the inception. It involves judicial oversight in the context of specific discovery disputes. Congress struck that balance purposefully, in light of a long and infamous history of abuse of electronic surveillance by the Executive branch in the name of national security.

*Second*, the Government has narrowed this litigation by emphasizing that the subject matter it now wants to protect is not a state secret. Specifically, the Assistant Attorney General has declared that the unrebutted record evidence submitted by Plaintiffs describing AT&T's participation in the NSA's dragnet electronic surveillance program is not subject to the state secrets privilege.

It is not permissible at this point to make predictions about the future course of this case. But even if it were, Plaintiffs will be able to prove their case without resort to state secrets. Indeed, they already have. The expert testimony—analyzing voluminous and detailed AT&T documents—alone suffices to establish that AT&T participated in the Government's massive communications dragnet. That is all Plaintiffs need to establish the *prima facie* case in support of most of their statutory claims.

Neither Plaintiffs' claims nor AT&T's defenses depend on how, why, when, or where the Government might use the communications or records AT&T divulges. Once AT&T discloses the communications or records to the Government, the *prima facie* case is established.

Plaintiffs' complaint includes more than sufficiently specific allegations setting forth the basis for their standing to pursue this action. Plaintiffs include AT&T customers whose internet and telephone traffic and communications records have been intercepted and disclosed to the NSA. Plaintiffs can prove these facts without resort to state secrets.

## **ARGUMENT**

### **I. THE STATE SECRETS PRIVILEGE IS A NARROW, EVIDENTIARY PRIVILEGE AND IS NOT AN IMMUNITY FROM SUIT.**

The state secrets privilege is an evidentiary privilege, not an absolute immunity from suit. As the Supreme Court has explained, the "privilege" is "well established *in the law of evidence.*" *United States v. Reynolds*, 345 U.S. 1, 7-8 (1953) (emphasis added). This Court has found that the privilege therefore never warrants dismissal at the pleading stage except in one very narrow circumstance: "if the 'very subject matter of the action' is a state secret." *Kasza v. Browner*, 133 F.3d 1159, 1166 (9th Cir. 1998) (quoting *Reynolds*, 345 U.S. at 11 n.26). In light

of this demanding standard, it is no surprise that the courts almost never dismiss a case at the pleading stage based on the privilege.

The Supreme Court's seminal opinion on the state secrets privilege, *United States v. Reynolds*, illustrates the point. The case was a tort suit against the Government for the deaths of three civilians in the crash of a military aircraft. They were on board to observe the testing of secret electronic equipment. 345 U.S. at 2-3. To prove their case, the plaintiffs sought several specific pieces of evidence, including "the Air Force's official accident report." *Id.* The Government resisted, "assert[ing] that the demanded material could not be furnished 'without seriously hampering national security.'" *Id.* at 5. The Supreme Court agreed. *Id.* at 10.

The Supreme Court did not, however, dismiss the case. As much as the Government might have preferred to insulate itself *entirely* from litigation about the secret mission and the cause of the crash, the Court observed that the case raised only a "question of the Government's privilege to resist discovery." *Id.* at 3. The Court hypothesized that "it should be possible for [the plaintiffs] to adduce the essential facts as to causation without resort to material touching upon military secrets." *Id.* at 11. And the Court remanded the case to give the plaintiffs the opportunity to try to do just that. *Id.* at 12. This was not a case, the Court noted, "where the very subject matter of the action . . . was a matter of state secret."

*Reynolds*, 345 U.S. at 11 n.26 (distinguishing *Totten v. United States*, 92 U.S. 105, 107 (1875)).

In the half-century since *Reynolds*, the courts have consistently followed the Supreme Court’s lead in applying the state secrets privilege to discrete and concrete evidentiary or discovery disputes.<sup>3</sup> Over the decades, the Government has tried, as it does here, to leverage the evidentiary privilege into an absolute immunity from suit, to derail a suit at the pleading stage. But the courts have routinely rebuffed the Government’s efforts.

One example is *In re United States*, 872 F.2d 472 (D.C. Cir. 1989). There, as here, the plaintiff sought damages alleging a pattern of illegal domestic surveillance by the Government (involving the FBI’s notorious COINTELPRO surveillance program). *Id.* at 473. Just as it does here, the Government there

---

<sup>3</sup> See, e.g., *Northrop Corp. v. McDonnell Douglas Corp.*, 751 F.2d 395, 396 (D.C. Cir. 1984) (privilege invoked in response to a subpoena *duces tecum* against the Departments of Defense and State); *Linder v. Nat’l Sec. Agency*, 94 F.3d 693, 694 (D.C. Cir. 1996) (privilege invoked in response to a subpoena *duces tecum* against the NSA); *Molerio v. FBI*, 749 F.2d 815, 819 (D.C. Cir. 1984) (privilege invoked in response to motion to compel); *In re Under Seal*, 945 F.2d 1285, 1287 (4th Cir. 1991) (privilege invoked “[a]fter several depositions and other preliminary matters were conducted,” in response to a “motion to compel answers to [deposition] questions”); *DTM Research L.L.C. v. AT&T Corp.*, 245 F.3d 327, 330 (4th Cir. 2001) (privilege invoked in response to particular discovery requests); *Bowles v. United States*, 950 F.2d 154, 156 (4th Cir. 1991) (privilege invoked in response to plaintiffs’ discovery requests); *Heine v. Raus*, 399 F.2d 785, 787 (4th Cir. 1968) (privilege invoked during discovery).

sought to cut off the case at the threshold. *Id.* at 473-74. In a plea that echoes throughout the Government’s brief here, the Government there swore that “any further discovery in this action will occasion . . . ‘disclosures [that] . . . would . . . cause serious damage to the national security.’” *Id.* at 480 (Ginsburg, J., concurring and dissenting) (quoting F.B.I. affidavit). The D.C. Circuit refused to dismiss, rejecting the Government’s effort to inflate a “*common law evidentiary rule* that protects information from discovery” into an immunity from suit. *Id.* at 474 (emphasis added). “Dismissal of a suit, and the consequent denial of a forum without giving the plaintiff her day in court,” the court held, “is indeed draconian”—“a drastic remedy that has rarely been invoked.” *Id.* at 477 (quoting *Fitzgerald v. Penthouse Int’l, Ltd.*, 776 F.2d 1236, 1242 (4th Cir. 1985)). The court held that “broad application of the privilege to all of [the Government’s] information, before the relevancy of that information has even been determined, was inappropriate at this early stage of the proceedings.” *Id.* at 478. *See also Clift v. United States*, 597 F.2d 826, 827-30 (2d Cir. 1979) (rejecting Government’s plea to dismiss case on state secrets grounds, because plaintiff “has not conceded that without the requested documents he would be unable to proceed, however difficult it might be to do so”).

This holding is consistent not only with the Supreme Court’s teaching, but with numerous other court of appeals cases drawing the same distinction.<sup>4</sup> These cases teach that it is not enough for the Government to assert (as it does here) “that privileged information lies at the core of this case, which affects both the plaintiff’s ability to establish her claims and the government’s ability to defend itself.” *In re United States*, 872 F.2d at 477. Nor will it suffice for the Government to argue that “continuation of plaintiff’s action will *inevitably* result in disclosure of information that will compromise current foreign intelligence and counterintelligence investigative activities.” *Id.* at 477 (emphasis added); *see Clift*, 597 F.2d at 828. Rather, the courts of appeals have insisted that so long as it is conceivable that the case could proceed without forcing the Government to divulge state secrets, the case must proceed. *Clift*, 597 F.2d at 830. The D.C. Circuit captured the pervasive sentiment in one curt sentence: “We share the district court’s confidence that it can police the litigation so as not to compromise national security.” *In re United States*, 872 F.2d at 480.

---

<sup>4</sup> *See Crater Corp. v. Lucent Techs., Inc.*, 423 F.3d 1260, 1268-69 (Fed. Cir. 2005) (reversing dismissal after recognizing certain information was protected by state secrets privilege because record was not sufficiently developed to determine that claims could not proceed without excluded evidence); *Monarch Assurance P.L.C. v. United States*, 244 F.3d 1356, 1364 (Fed. Cir. 2001) (holding dismissal was “premature” after district court concluded certain evidence was privileged from discovery because plaintiff should be afforded opportunity to make its case without privileged evidence).

## II. THE DISTRICT COURT CORRECTLY CONCLUDED THAT THE VERY SUBJECT MATTER OF THIS SUIT IS NOT A STATE SECRET.

All the parties agree that the subject matter of this action is whether AT&T participated in an illegal program of electronic surveillance. *See* Gov. 10. This is how the Government characterizes the secret: “Whether AT&T is involved in . . . the broad[] activities alleged by plaintiffs is a state secret that neither the Government nor AT&T can confirm or deny.” Gov. 10. The Government cannot demonstrate, as it must to secure a dismissal, that this entire “‘subject matter’ . . . is a state secret,” *Kasza*, 133 F.3d at 1166 (citing *Reynolds*, 345 U.S. at 11 n.26), or, stated another way, that “the *whole object* of the suit and of the discovery is to establish a fact that is a state secret,” *Molerio*, 749 F.2d at 821 (emphasis added).<sup>5</sup>

The Government’s effort to satisfy this demanding standard fails for two independent reasons. First, and conclusively, Congress has determined that cases concerning electronic surveillance conducted in the name of national security

---

<sup>5</sup> Under the law of this Circuit, cases may be dismissed at the inception under the circumstances described in the text. *See infra* pp. 45-55; *Kasza*, 133 F.3d at 1166. In support of that proposition, this Court has cited *Totten*, 92 U.S. at 107. However, more recent Supreme Court precedent clarifies that this rule does not apply in the usual state secrets case. *Tenet v. Doe*, 544 U.S. 1, 8-9 (2005). *Tenet* indicates that such a dismissal on the pleadings may only be available where the *Totten* jurisdictional bar applies—*i.e.*, where “alleged spies” bring claims “where success depends upon the existence of their secret espionage relationship with the government.” *Id.* at 8. We nevertheless apply the “subject matter” dismissal doctrine of *Kasza* because this Court has never had the opportunity to reconsider it in light of *Tenet*.

should be subject to FISA, which *does* require the court to review alleged state secrets under certain circumstances and *prohibits* dismissal at the outset. *See infra* Point II.A. Second, and independently, the subject matter is not a state secret because it is simply not a secret. *See infra* Point II.B. Either point defeats the Government’s effort to dismiss this case. None of the cases the Government and AT&T invoke supports their position. *See infra* Point II.C. And they fail to acknowledge the constitutional ramifications of interpreting a common law doctrine to prohibit a court from even considering a case with allegations of widespread warrantless surveillance of millions of Americans. *See infra* Point II.D.

**A. Congress Has Determined that the Very Subject Matter of this Case Is Not a State Secret that Warrants Dismissal.**

Where Congress “speaks *directly* to the question otherwise answered by . . . common law”—including the question of how to handle state secrets in litigation—Congress’s judgment binds both the Executive and the Courts. *Kasza*, 133 F.3d at 1167 (internal citation and brackets omitted). Congress has spoken “directly to the question” presented in this case, and directed that dismissal on the pleadings is impermissible.

**1. Congress has directed the procedure for assessing claims of national security in electronic surveillance cases, and does not allow dismissal on the pleadings.**

As part of FISA, Congress commanded that the procedures of FISA and Title III are the “*exclusive means* by which electronic surveillance . . . and the interception of domestic . . . communications may be conducted.” Pub. L. No. 95-511, 92 Stat. 1783, § 201 (1978), codified as amended at 18 U.S.C. § 2511(2)(f) (emphasis added). Congress gave these requirements teeth by authorizing anyone who has been subjected to illegal electronic surveillance to bring lawsuits like this one.<sup>6</sup>

Congress did not merely create causes of action for illegal surveillance. Obviously, when Congress authorized these sorts of lawsuits, it expected that some would implicate “Foreign Intelligence Surveillance.” It also expected that any FISA lawsuit against a private party like AT&T would require proof of “the relationship, if any, between AT&T and the Government,” Gov. at 2; that is what it means to prove that a private entity acted “under color of law.” 50 U.S.C. § 1809(a).

---

<sup>6</sup> See 18 U.S.C. §§ 2520(a) (civil cause of action for interception of communications in violation of Title III); 50 U.S.C. § 1810 (same for electronic surveillance in violation of FISA); see also 18 U.S.C. § 2707(a) (same for unlawful disclosures by communications providers under SCA); 50 U.S.C. § 1809 (prohibiting “electronic surveillance under color of law except as authorized by statute”); 47 U.S.C. § 605(e)(3)(A) (same for unlawful disclosures by communications providers under Communications Act).

Even at the most basic level, then, the Government’s position is at war with the very premise of FISA. Its position is that Congress authorized lawsuits to challenge unlawful intelligence-gathering collaborations with the Government, but allowed the Government to scuttle any such suit at the inception by declaring that the very existence of any such relationship is a secret.

Congress was not that obtuse. It prescribed exactly what must happen where “an aggrieved person” (like Plaintiffs here) files a lawsuit (like this one), and the Executive intervenes (as it did here) and “files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States.” 50 U.S.C. § 1806(f). The answer is not, as the Government here demands, that the lawsuit gets dismissed at the outset. Congress’s lengthy and detailed answer, codified in Section 1806(f), is:

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

*Id.* (emphasis added).

With Section 1806(f), Congress made two basic judgments. The first judgment reflected Congress’s substantive view of the “subject matter” of electronic surveillance. Congress determined that in any case where the legality of electronic surveillance is challenged, there could be circumstances in which “the court may disclose to the aggrieved person” information that the Government maintains “would harm the national security.” Disclosure is not mandated, but nor is it *per se* prohibited. Put otherwise, Congress has decreed that every such case begins with the *potential* that at some point a court may order that *some* information concerning electronic surveillance conducted for national security purposes may be divulged (always “under appropriate security procedures”).

That substantive judgment reflects a balance of national security against the need to provide for meaningful private causes of action against illegal electronic surveillance—and it is fatal to the Government’s position here. In any challenge to electronic surveillance there is the potential that information that the Government contends is subject to the state secret privilege *might* be disclosed. Given that reality, the Government simply cannot claim that *all* information related to the subject matter of national security electronic surveillance must be kept secret.

Congress’s second judgment was procedural. Congress required the Executive and the Courts, alike, to follow a five-step protocol whenever a claim of state secrets privilege arises in the context of litigation over electronic

surveillance—a process crafted to afford a plaintiff the chance to make his or her case while still protecting the Government’s legitimate claims of national security.

The five-step protocol is as follows:

1. The court must await a “motion or request . . . by an aggrieved person . . . to discover or obtain . . . materials relating to electronic surveillance.” 50 U.S.C. § 1806(f).
2. Once that request comes, “the Attorney General [may] file[] an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States.” *Id.*
3. Upon receipt of that affidavit, the “court . . . shall . . . review in camera and *ex parte*” any materials about the surveillance “as may be necessary [to allow the court] to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted.” *Id.*
4. Based upon that submission, the court decides whether to “disclose to the aggrieved person” any “materials relating to the surveillance”—a step that is permissible “only where such disclosure is necessary to make an accurate determination of the legality of the surveillance.” *Id.*
5. If the court concludes that disclosure to the plaintiff is necessary, the court discloses the materials along with “appropriate security procedures and protective orders” to limit the national security risk. *Id.*

In the end, whether or not the materials relating to the surveillance are disclosed to the plaintiff, the Court must “determine whether the surveillance of the aggrieved person was lawfully authorized and conducted.” *Id.* Absent from this five-step protocol is any authorization for the relief the Government demands here; Congress did not authorize the Executive to obtain dismissal by preemptively declaring that the entire subject matter of an action was a state secret.

These two congressional judgments mean that in electronic surveillance cases it can never be said, *ex ante*, that the very subject matter is a state secret warranting dismissal. This is why the Conference Report for the statute enacting Section 1806(f) noted that “the conferees also agree that the standard for disclosure in the Senate bill adequately protects the rights of the aggrieved person, and that the provision for security measures and protective orders ensures adequate protection of national security interests.” H.R. Conf. Rep. No. 95-1720, at 32 (1978), *as reprinted in* 1978 U.S.C.C.A.N. 4048, 4061; *see also* S. Rep. No. 95-701, at 64 (1978), *as reprinted in* 1978 U.S.C.C.A.N. 3973, 4033 (calling Section 1806(f) “a reasonable balance between an entirely in camera proceeding . . . and mandatory disclosure, which might occasionally result in the wholesale revelation of sensitive foreign intelligence information”).

The statutes governing electronic surveillance, then, contain exactly the sort of explicit legislative direction this Court has held would be necessary to supersede the common law privilege. *See Kasza*, 133 F.3d at 1167. On the one hand, this Court held that Congress does not supersede the privilege merely by creating a cause of action. *Id.* On the other hand, where, as here, one can “discern . . . Congressional intent to replace the government’s evidentiary privilege to withhold sensitive information” with a different protocol, the common law rules must yield to legislative strictures. *Id.* at 1168.

**2. Congress struck that balance because it did not want the Executive to shield illegal surveillance with sweeping assertions of national security.**

Congress superseded the common law state secrets privilege with Section 1806(f)'s five-step protocol for a reason: "to curb the practice by which the executive branch may conduct warrantless electronic surveillance on its own unilateral determination that national security justifies it." S. Rep. No. 95-604(I), at 8 (1978), *as reprinted in* 1978 U.S.C.C.A.N. 3904, 3910.

FISA was Congress's response to the 1976 findings of the United States Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, known informally as the "Church Committee," after its Chairman, Sen. Frank Church. The Church Committee revealed "that warrantless electronic surveillance in the name of national security ha[d] been seriously abused." S. Rep. No. 95-604 (I), at 7-8 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3904, 3908-09; *see* S. Select Comm. to Study Governmental Operations with Respect to Intelligence Activities, 94th Cong., S. Rep. No. 94-755 (1976) (Church Committee Books I-VI), *available at* <http://www.aarclibrary.org/publib/church/reports/contents.htm>; *see also* *United States v. Belfield*, 692 F.2d 141, 145-46 (D.C. Cir. 1982) (discussing FISA's history).

The Church Committee was particularly troubled by the Executive's invocation of broad labels like "national security" to justify warrantless surveillance and insulate it from judicial review:

The application of vague and elastic standards for wiretapping and bugging has resulted in electronic surveillances which, by any objective measure, were improper and seriously infringed the Fourth Amendment rights of both the targets and those with whom the targets communicated.

Church Committee Book III at 332. The Church Committee concluded that "[t]he Constitutional system of checks and balances ha[d] not adequately controlled intelligence activities," Church Committee Book II at 6, and recommended that the NSA be limited by "a precisely drawn legislative charter," *id.* at 309. *See generally* Civil Rights Organization Br. (recounting abuses revealed by Church Committee); People for the American Way Br. (recounting other steps Congress took to constrain the Executive).

The Executive cannot upend the balance Congress struck by asserting an extra-statutory formulation of the state secrets privilege that Congress rejected for these very sorts of lawsuits. Nor can the Executive scuttle a lawsuit that Congress expressly anticipated with the blithe assertion that the entire subject matter is beyond judicial review. "When the President takes measures incompatible with the express or implied will of Congress, his power is at its lowest ebb, for then he can rely only upon his own constitutional powers minus any constitutional powers

of Congress over the matter.” *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 637 (1952) (Jackson, J., concurring), *quoted with approval in* H.R. Conf. Rep. 95-1720, at 35 (1978), *as reprinted in* 1978 U.S.C.C.A.N. 4048, 4064.

**3. FISA’s procedure for handling state secrets applies to this case.**

There is no basis for ignoring Congress’s mandate in this case.

First, the Government wrongly argues that Plaintiffs are not “aggrieved persons,” within the meaning of Section 1806(f), because they cannot prove at the outset of the case that they were the *targets* of surveillance. Gov. 29. An “aggrieved person” is a “target of an electronic surveillance *or any other person whose communications or activities were subject to electronic surveillance.*” 50 U.S.C. § 1801(k) (emphasis added).<sup>7</sup> Plaintiffs have sufficiently alleged—indeed, demonstrated—that they fall into the latter category. For reasons more fully explained below, *see infra* pp. 69-75, in order to survive a motion to dismiss, Plaintiffs need not prove definitively at the pleadings stage that any particular communication was, in fact, intercepted in order for the procedures of Section 1806(f) to apply. *See ACLU Foundation of Southern Cal. v. Barr*, 952 F.2d 457, 469 (D.C. Cir. 1991).

---

<sup>7</sup> Cases cited by the Government holding that a party fell within the definition because he *was* a “target of an electronic surveillance,” *see, e.g., United States v. Ott*, 827 F.2d 473, 475 n.1 (9th Cir. 1987), *cited in* Gov. 29, never suggest that this would be the only way to satisfy the definition.

Second, contrary to the position the Government took below, the five-step protocol FISA prescribes for handling state secrets is not limited to an effort to suppress the fruits of illegal electronic surveillance evidence in a criminal prosecution (or other Government action). Section 1806(f) applies also to a *civil* suit brought by *private* parties. Congress prescribed that its protocol must be followed:

*whenever any motion or request is made by an aggrieved person pursuant to any . . . statute or rule of the United States or any State before any court or other authority of the United States or any State to discover or obtain applications or orders or other materials relating to electronic surveillance.*

50 U.S.C. § 1806(f) (emphasis added); *see Barr*, 952 F.2d at 462.

Third, this five-step protocol applies to all of Plaintiffs' statutory and constitutional claims, not just claims for FISA violations. Section 1806(f) is not limited to certain classes of claims. "When a district court conducts a § 1806(f) review, its task is not simply to decide whether the surveillance complied with FISA. Section 1806(f) requires the court to decide whether the surveillance was 'lawfully authorized and conducted.'" *Barr*, 952 F.2d at 465; *id.* at 465 n.7. Section 1806(f) provides, without qualification, that it applies to all "electronic surveillance," which is defined to encompass any "acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication . . . without the consent of any party thereto." 50 U.S.C.

§ 1801(f)(2). The protocol also covers communications records because “contents” is defined to include “any information concerning the *identity of the parties* to such communication or the *existence*, substance, purport, or meaning of that communication.” 50 U.S.C. § 1801(n) (emphasis added); *compare* 18 U.S.C. § 2510(8) (narrower definition of contents for purposes of Wiretap Act). Information concerning AT&T’s disclosure of communications records is also subject to Section 1806(f) because such information is “material[] relating to the surveillance.” 50 U.S.C. § 1806(f).

Finally, the Government alludes to three statutes which (at least before the District Court) it invoked in support of its argument that Section 1806(f)’s procedures have been superseded in the context of this case. *See* Gov. 23-24, 42 n.2 (citing Authorization of the Use of Military Force Act, Pub. L. No. 107-40, 115 Stat. 224 (2001); 50 U.S.C. § 402 note; 50 U.S.C. § 403-1(i)(1)). None of those statutes provides a mechanism by which illegal surveillance can be litigated. The more specifically drawn FISA statute must prevail over these more general statutes in governing electronic surveillance. *See Edmond v. United States*, 520 U.S. 651, 657 (1997).

\* \* \*

In sum, Congress has spoken clearly on the topic of how to handle claims of state secrets privilege in the context of litigation over illegal electronic

surveillance. Congress did not mandate any specific disclosure. But it did mandate a protocol that does not include dismissal of cases. In insisting that the entire subject matter is secret, the Government is asking this Court to do exactly what Congress prohibited—to substitute Executive fiat for careful judicial review.

**B. The Very Subject Matter of this Suit Is Not a Secret.**

There is a second, independent reason why the Government cannot succeed in demonstrating that the very subject matter of this case is a state secret: AT&T's collaboration in the Government dragnet—both as to the interception of communications and as to the disclosure of communications records—is simply not a secret. See *Capital Cities Media, Inc. v. Toole*, 463 U.S. 1303, 1306 (1983) (noting Court has not “permitted restrictions on the publication of information that would have been available to any member of the public”); *McGehee v. Casey*, 718 F.2d 1137, 1141 (D.C. Cir. 1983) (noting “[t]he government has no legitimate interest in censoring unclassified materials” or “information . . . derive[d] from public sources”). As to the interception of communications, Plaintiffs have already adduced enough evidence to prove that AT&T collaborated with the NSA's efforts, and the Government has made a considered judgment that this evidence is not a state secret. See *infra* Point II.B.1. This concession was correct. See *infra* Point II.B.2. As to the wholesale disclosure of communications records, the public

statements of public officials and telecommunications carriers have long since exposed the surveillance efforts to the full light of day. *See infra* Point II.B.3.

**1. The evidence already submitted establishes that AT&T collaborated with the NSA in electronic surveillance, and the Government has conceded that the evidence is not a state secret.**

For reasons already discussed, Plaintiffs are entitled to further discovery (subject to the protocol of Section 1806(f)) before dismissal can even be contemplated. But even without any more, the declarations and AT&T schematics already adduced demonstrate that AT&T has been collaborating with the NSA in a massive program of electronic surveillance. Mr. Klein has attested to the fact that AT&T has set aside a special room that is accessible only to the NSA. SER 4. He has explained how AT&T split a fiber optic cable to divert all peered internet traffic into that room. SER 5-6. Telecommunications expert Mr. Marcus has painstakingly explained why the only function that could possibly be served by this diversion is a massive program of electronic surveillance. SER 148-51. In short, the basic subject matter of this case—AT&T’s collaboration in a massive electronic surveillance program—has been established with the non-secret evidence already adduced. (As is demonstrated below, the evidence already adduced also establishes a *prima facie* case for most of Plaintiffs’ claims, *see infra* pp. 60-64, even though Plaintiffs need not sustain any such burden in order to

defeat the Government's argument that the *very subject matter* of this suit is a state secret.)

To ascertain that this central point is not a state secret, the Court need look no further than the pronouncement of Assistant Attorney General Peter Keisler in open court:

First of all, with respect to the suggestion that the plaintiffs already put forward a prima facie case. They note correctly that we haven't said any documents are classified. They say we can't now unring that bell. We don't want to unring that bell. *None of the documents they have submitted to accompany these declarations implicate any privileged matters.*

THE COURT: Including the Klein documents[?]

MR. KEISLER: *We have not asserted any privilege over the information that is in the Klein and Marcus declarations.*

THE COURT: *Either the declaration or its exhibits?*

MR. KEISLER: *We have not asserted a privilege over either of those.*

AER 189 (emphasis added); *see Hepting*, 439 F. Supp. 2d at 989. The only reason that these key declarations remain under seal is because AT&T has designated them proprietary trade secrets. *See* SER 508-09. As far as the Government is concerned, it would have been perfectly fine for Plaintiffs to post these documents on the internet or hand them to *USA Today*. At a minimum, by conceding that “none of the *documents* . . . implicate any privileged matters,” the Government has waived any objection to Plaintiffs' intention to prove the truth of the facts

contained in those declarations and exhibits and to persuade a fact-finder to draw reasonable inferences from them.

The Government is not free to retreat from its concession now. This was not an idle and ill-considered quip from a functionary. It was a pronouncement from the highest Executive official on the case. Moreover, he gave the point primacy—these were the first words out of his mouth when he stood up to articulate the Government’s position—precisely because the point was central to the Government’s strategy. The Government needed to fend off Plaintiffs’ compelling argument that it was trying to censor information that was already in the public domain—to “unring th[e] bell” of the Klein revelations. AER 189. The Government made the considered judgment not to take such an aggressive stance, but to limit its litigation posture to the proposition that this case cannot proceed even though Plaintiffs are free to prove every fact contained in the Klein and Marcus declarations and the AT&T schematics. Having conceded that the contents of these materials are not state secrets, the Government cannot now insist that the entire subject matter of this case is a state secret.

## **2. The Government’s concession was correct.**

The Government’s concession was not only binding, but correct. The law permits Plaintiffs to rely on information received from non-governmental sources to demonstrate that the very subject matter of this suit is not a state secret. In

arguing otherwise, the Government is now taking the position that it can, indeed, somehow “unring that bell.” The Government’s theory is that it can invoke the state secrets privilege to prevent Plaintiffs from proving a fact based upon non-classified information they have obtained entirely from non-governmental sources, just because the Government does not want that non-secret fact proven in a court of law.

That position runs headlong into this Court’s direction on how the state secrets privilege is supposed to work: “First, by invoking the privilege over particular evidence, the evidence is completely removed from the case. *The plaintiff’s case then goes forward based on evidence not covered by the privilege.*” *Kasza*, 133 F.3d at 1166 (emphasis added). The Government cites no case holding that it may block a plaintiff from proving a fact established by information already in the public arena—much less a case holding that the Government can block a plaintiff from proving a fact from information the Government concedes is non-classified and not itself secret.

The one case the Government invokes in support of this proposition holds no such thing. Specifically, the Government quotes *Bareford v. General Dynamics Corp.*, 973 F.2d 1138, 1144 (5th Cir. 1992), arguing: “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-governmental sources.” Gov. 21. Those words do, indeed, appear in the Fifth Circuit’s opinion, but the court was simply recounting the *Government’s* position. In the very next sentence, the court observed that “[t]his contention has a troubling sweep.” 973 F.2d at 1144. The court then said, “we do not rest upon it, because we need not.” *Id.*

In any event, even if that position were the law, it would not help the Government here. It is one thing to assert (as the Government did in *Bareford*) that “disclosure of information *by government officials*” could harm national security even if the information has entered the public arena. Gov. 21 (emphasis added). The point there was that “acknowledgment of . . . information by government officers . . . would lend credibility to the unofficial data” pieced together from the public record. *Bareford*, 973 F.2d at 1144. But that is not what the Government is guarding against here. Here, the Government seeks to prevent Plaintiffs from proving a fact entirely from information already available in the public arena, even though that fact can be proven without the Government’s official confirmation of its truth.

For similar reasons, the Government and AT&T do not advance their position by invoking the principle that “the state secrets privilege ‘belongs to the Government’ and cannot be ‘waived by a private party.’” Gov. 21 (citing *Reynolds*, 345 U.S. at 7, and other cases); *see also* AT&T 21. When the Supreme

Court held that the state secrets privilege “can neither be claimed nor waived by a private party,” *Reynolds*, 345 U.S. at 7, it obviously did not mean that a plaintiff must prove his case only with testimony from governmental sources. In *Reynolds* itself, the Supreme Court allowed the plaintiffs to try to prove their case with testimony and evidence from non-governmental sources. Rather, this rule merely means that the privilege belongs to the Government, and a private party to the litigation—here, AT&T—can neither assert nor waive the state secrets privilege on the Government’s behalf. *See* Wright & Graham, 26 Fed. Prac. & Proc. § 5665 (“[T]he secrecy required for the privilege can be destroyed without regard to who made or authorized the disclosure.”).

The District Court, for its part, had a different reason for declining to consider the Klein declaration and supporting materials, even though Mr. Klein’s “assertions would appear admissible.” *Hepting*, 439 F. Supp. 2d at 990. Its rationale was prophylactic. To consider such evidence here, the court worried, “would invite attempts [in other cases] to undermine the privilege by mere assertions of knowledge by an interested party.” *Id.* That is incorrect. What Plaintiffs adduced, in the form of both firsthand sworn observations by a former AT&T employee who is not a party to this litigation as well as AT&T’s own schematic diagrams, were not “mere assertions of knowledge by an interested party.” But even if they were, to allow such evidence to defeat a motion to dismiss

could not “undermine the privilege.” The only way to “undermine the privilege” would be to use baseless allegations to pry a secret *out of the Government*.

Plaintiffs have sought no such result here.

**3. Public statements by Government officials and others confirm that disclosure of communications records to the Government is not a secret.**

AT&T’s participation in the Government’s efforts to collect communications *records* is no more secret than its collaboration in the Government’s efforts to intercept communications. While these efforts are not described in Mr. Klein’s declaration, they have been described by sources that are at least as reliable: members of Congress (at least 19 of them) who have been briefed by the Executive Branch and other telecommunications carriers whom the Government has also approached. *See supra* pp. 10-13; *Spock v. United States*, 464 F. Supp. 510, 520 (S.D.N.Y. 1978) (“Here, where the only disclosure in issue is the admission or denial of the allegation that interception of communications occurred[,] an allegation which has already received widespread publicity[,] the abrogation of the plaintiff’s right of access to the courts would undermine our country’s historic commitment to the rule of law”).

With these facts splayed across the front pages of newspapers, and with new public admissions continuing to be made (as recently as two weeks before this

brief was submitted), the District Court was correct that dismissal of the communications records claims was improper.

Despite this evidence, the District Court incorrectly limited its review to *Executive and telecommunications carrier* admissions in determining whether the surveillance was still a secret. *Hepting*, 439 F. Supp. 2d at 990. By limiting its consideration to those two narrow categories, and by refusing to find sufficient the record admissions of other telecommunications carriers, *see id.* at 997, the District Court determined that the communications records claims in the case must await some yet further public confirmation.

In this, the District Court erred. Federal Rule of Evidence 104(a) provides that in considering whether a privilege exists, the court is “not bound by the rules of evidence except those with respect to privilege,” and may consider any evidence which makes the preliminary fact “more likely than not.” *Bourjaily v. United States* 483 U.S. 171, 175 (1987). The Supreme Court has applied this approach in the state secrets context, requiring courts not merely to consider governmental admissions, but to consider “all the evidence and circumstances” in determining whether the privilege applies. *Reynolds*, 345 U.S. at 9; *see also supra* pp. 39-43. Here, “all the evidence and circumstances” includes the massive record of public acknowledgements, from the front pages of major newspapers to the halls of Congress, all of which support the conclusion that the disclosure of

communications records is not a secret. Not only should the communications records claims survive dismissal, they should be allowed to proceed.

**C. This Case Is Distinguishable from Decisions in which the Entire Subject Matter of the Action Was a State Secret and Where the Case Was Dismissed After Discovery.**

The points discussed above distinguish this case from the rare situations in which the courts have dismissed at the inception on the ground that the very subject matter of the case was a state secret. The Government cannot point to a single case in which a court dismissed a complaint at the inception on state secrets grounds despite a congressional command that state secrets be handled in a different way. And there certainly is no decision dismissing a case on that ground where plaintiffs have put forward unrebutted, sworn testimony to prove their claims and the Government has conceded that the testimony is not subject to the state secrets privilege.

Nevertheless, the Government and AT&T invoke several opinions in which cases were dismissed on the pleadings under other circumstances. First, they invoke the so-called “*Totten* bar.” *See infra* Point II.C.1. Then, they cite a handful of decisions from the courts of appeals dismissing cases at the outset. *See infra* Point II.C.2. For good measure, they cite opinions where the case was dismissed only after extensive discovery confirmed that the plaintiffs could not prove their

case without access to state secrets. *See infra* Point II.C.3. All these cases are distinguishable.

**1. This case is not subject to the *Totten* bar.**

Invoking the Supreme Court’s opinion in *Totten*, 92 U.S. at 107, and a subsequent application of *Totten* in *Tenet v. Doe*, 544 U.S. 1, 8 (2005), the Government argues 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.” Gov. 17. The Government is wrong.

The plaintiff in *Totten* was a spy—or, at least, he claimed to be one.<sup>8</sup> The suit alleged that the Government had hired him as a spy during the Civil War but had not paid him adequately. 92 U.S. at 105. The only issue in the case was whether the avowed spy had entered into “a contract for secret services” with the Government. *Id.* at 107. The Court dismissed the lawsuit because there was no way for the purported spy to win his claim for money without breaching his vow of confidentiality and proclaiming publicly that he was a spy. *Id.*

In *Tenet v. Doe*, the Supreme Court applied the “*Totten* bar” to dismiss another case—also brought by former spies. 544 U.S. at 3. There, the avowed

---

<sup>8</sup> More accurately, it was the purported spy’s executor who brought the suit, standing in the spy’s shoes.

spies alleged that the Government violated their constitutional rights by suspending financial assistance it had allegedly promised them. *Id.* at 5. The Supreme Court reiterated that “*Totten* precludes judicial review in cases such as [the spy plaintiffs’] where success depends upon the existence of their secret espionage relationship with the Government.” *Id.* at 8.

From these cases, the Government concludes that no suit should ever be allowed to proceed if it is designed to demonstrate that a private party has a secret relationship with the Government. *See* Gov. 17. The Government’s argument that this case must be dismissed under *Totten* and *Tenet* fails for two basic reasons.

First, as the District Court recognized, *Totten* and *Tenet* are reserved for cases in which spies themselves sue the Government. *See Hepting*, 439 F. Supp. 2d at 991. That is what the Supreme Court meant when it said that “[n]o matter the clothing in which *alleged spies dress their claims*, *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 (emphasis added). *Totten* bars spies from exposing to the world *their own* secret relationship to advance their personal economic interests. *See Hepting*, 439 F. Supp. 2d at 991. Thus, *Totten* and *Tenet* might mean that *AT&T* could not sue the Government to recover more money in connection with the surveillance it was

doing. But they certainly do not mean that victims of the illegal spying cannot use non-secret information to prove either the collaboration, or harm from it.

Second, in *Totten* and *Tenet*, the Court was applying a common law privilege in a context that Congress had not occupied. Congress has never crafted an Avowed Spy Compensation Act—a detailed statutory scheme providing for the litigation of claims by former spies against the Government. Congress certainly did not specify a multi-step protocol balancing the interest in protecting sensitive information (such as the existence of a secret espionage relationship) against the interest in having an effective cause of action. In asserting that *Totten* precludes lawsuits against private carriers who illegally conduct electronic surveillance under color of law, the Government is arguing that the Court’s application of federal common law somehow overrides the five-step protocol Congress specified in FISA for cases just like this, and the judgment that in any given electronic surveillance case some state secrets must be considered necessary to determine the legality of the surveillance, and may have to be divulged. It does not.

The Government does not succeed in extending the scope of the *Totten* bar by invoking *Weinberger v. Catholic Action of Hawaii/Peace Education Project*, 454 U.S. 139 (1981). *See* Gov. 19. *Weinberger* was an environmental lawsuit. The plaintiffs sought to compel the Navy to prepare and disclose an environmental impact statement for classified activities it was conducting. 454 U.S. at 142. The

Navy resisted, relying on statutes exempting from disclosure environmental impact statements involving the national defense. *Id.* at 144-45. In holding that these statutes foreclosed the plaintiffs’ cause of action against the Navy, the Court analyzed the “express intent of Congress manifested by the explicit language” in the relevant statutes. *Id.* at 144. The Court concluded that, in those statutes, “Congress has thus effected a balance between the needs of the public for access to documents prepared by a federal agency and the necessity of nondisclosure or secrecy. The Court of Appeals in this case should have accepted the balance struck by Congress . . . .” *Id.* at 145.

*Weinberger* cites to *Totten* for its general statement about the state secrets privilege—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, and respecting which it will not allow the confidence to be violated.” *Id.* at 146-47 (citing *Totten*, 92 U.S. at 107, and *Reynolds*, 345 U.S. 1 (cited in *Gov.* 19)). This statement has no bearing where, as here, Congress has struck a different balance that this Court must accept, and where “the law itself” provides a protocol for litigating plaintiffs’ claims.

**2. The handful of other opinions dismissing cases at the inception are also distinguishable.**

The Government and AT&T rely on a handful of cases that were dismissed at the pleadings stage because the very subject matter was a state secret. In each of

those cases, however, the plaintiff sought to prove such top-secret facts as precisely what spies do or precisely how secret weapons work. The very subject matter of this case does not involve proving any such secrets.

First, the Government and AT&T rely heavily on the Fourth Circuit's recent opinion in *El-Masri v. United States*, 479 F.3d 296 (4th Cir. 2007). The plaintiff there contended that the CIA and various unnamed CIA employees "were involved in a CIA operation in which [the plaintiff] was detained and interrogated" illegally. *Id.* at 299. The court dismissed the case because the plaintiff would have to delve into "the roles, if any, that the defendants played in the events he alleges." *Id.* at 309. "Such a showing could be made only with evidence that exposes how the CIA organizes, staffs, and supervises its most sensitive intelligence operations." *Id.* Acknowledging that dismissal at the pleading stage is rare, the Fourth Circuit dismissed the case because "sensitive military secrets w[ould] be so central to the subject matter of the litigation that any attempt to proceed w[ould] threaten disclosure of the privileged matters." *Id.* at 306 (quoting *Sterling v. Tenet*, 416 F.3d 338, 348 (4th Cir. 2005)).

Second, the Government relies on *Sterling v. Tenet*, 416 F.3d 338, 341 (4th Cir. 2005), in which the Fourth Circuit dismissed a CIA agent's claims of employment discrimination because they would have required him to present secret evidence about "the relative job performance of [CIA] agents, details of how

such performance is measured, and the organizational structure of CIA intelligence gathering.” *Id.* at 347.

In a third case, the estate of a sailor who was killed in combat sued defense contractors for negligence, claiming that the ship’s weapons systems were negligently designed, manufactured, and tested. *See Zuckerbraun v. Gen. Dynamics Corp.*, 935 F.2d 544, 546 (2d Cir. 1991). The court dismissed the case because the subject matter of the suit—the design and use of weapons systems—necessarily required discovery of the specifications for the weapons and defense systems aboard the ship as well as the procedures governing their use. *Id.* at 547-48. All of these details were state secrets. *Id.* The court noted that (unlike Plaintiffs here) the plaintiff “ha[d] not designated any sources of reliable evidence on the factual issues going to liability.” *Id.* at 548.

Unlike the plaintiffs in each of these cases, Plaintiffs here need not discover or prove the internal operations of any secret programs. There is no need here, as there was in *El-Masri*, for Plaintiffs to discover what roles any Government officials played in AT&T’s unlawful acts beyond demonstrating that AT&T was acting under color of law and as an agent of the Government. There is no need for Plaintiffs here to discover—as they had to in *El-Masri* and *Sterling*—how the Government “organizes, staffs, and supervises its most sensitive intelligence programs.” And there is no need here, as there was in *Zuckerbraun*, to divulge the

specification of secret weapons or intelligence procedures. Moreover, in none of these cases had Congress preempted the common law state secrets privilege with a detailed protocol for litigating cases using secret evidence as it has done here with FISA, 50 U.S.C. § 1806(f).

As will be demonstrated in even greater detail below, *see infra* pp. 60-64, Plaintiffs need not prove why the Government is interested in the communications and records AT&T unlawfully discloses to it, which communications within the dragnet the Government might target, or what the Government does with the intelligence it mines. All Plaintiffs have to prove is the unrevealing and well-known fact that AT&T intercepted or disclosed their communications and records—and did so without following statutory procedures. That is the subject matter of this suit and that subject matter is not a secret.

**3. Cases applying the state secrets privilege to specific discovery issues do not support dismissal on the pleadings.**

The Government and AT&T also rely heavily on decisions that have dismissed cases only after the discovery issues are joined, and it has become clear that a state secret is central to the defense or prosecution of a case. AT&T cites them for the proposition that “when it is apparent that the state secrets doctrine will prevent a court from fully and fairly adjudicating some element of a case that is essential to eventually reaching judgment, the case must be dismissed without further proceedings.” AT&T 28. To the contrary, those cases serve only to

underscore the impropriety of dismissing this case at the pleading stage. And of course, none of these cases featured a congressionally mandated protocol for *in camera* judicial resolution of state secrets issues.

A case in point is this Court’s opinion in *Kasza*, 133 F.3d 1159, which the Government features prominently. There, this Court did dismiss a case on the basis of the Government’s state secrets privilege. But the dismissal was not at the pleading stage. The district court addressed the state secrets issue on summary judgment, and only after the Government demonstrated to the district court that it was appropriate to block discovery specifically “with respect to the disclosure of certain categories of national security information.” *Id.* at 1163. This Court agreed summary judgment was appropriate, only because it first concluded that Congress had not modified the role of the state secrets privilege in the statutes giving rise to the plaintiff’s claims and only because “after further proceedings”—discovery and summary judgment motions—it became clear that the “plaintiff cannot prove the *prima facie* elements of her claim with nonprivileged evidence.” *Id.* at 1166.

For the same reasons, the Government can find no support in *Ellsberg v. Mitchell*, 709 F.2d 51 (D.C. Cir. 1983), and the two *Halkin* decisions—*Halkin v. Helms*, 598 F.2d 1 (D.C. Cir. 1978) (“*Halkin I*”), and *Halkin v. Helms*, 690 F.2d 977 (D.C. Cir. 1982) (“*Halkin II*”). All three cases concerned events occurring

before the enactment of FISA. In each, the parties had conducted extensive discovery. In *Halkin I*, the court remanded the case for further proceedings to determine whether the plaintiffs could prosecute some of their claims without resort to suppressed evidence. 598 F.2d at 11. And in *Halkin II* the court concluded they could not, but only after six years of discovery. 690 F.2d at 985. Likewise, in *Ellsberg*, the issue arose only after the plaintiffs had submitted interrogatories to the Government defendants, asking for “detailed information” regarding the wiretaps at issue and receiving an admission as to two wiretaps. 709 F.2d at 53. The court scrutinized the application of the privilege to specific evidence, and held that only partial dismissal was necessary. *Id.* at 52. *See also Fitzgerald*, 776 F.2d at 1243 (holding that “the very subject of this litigation is itself a state secret,” but only on the eve of trial, and only because the plaintiff made it clear that the only way he could prove his case was by “call[ing] expert witnesses with knowledge of relevant military secrets”).

As the court below well understood, these holdings do not add up to a license to (1) dispense with all discovery; (2) absolve the Government of any obligation to demonstrate to the court that the state secrets privilege is warranted as to each item sought; (3) preclude Plaintiffs from gathering evidence of a *prima facie* case in due course through alternative sources; or (4) dispense with the requirement of letting the case “go[] forward based on evidence not covered by the

privilege” and only then assessing, on the basis of a full record, whether “sensitive information [could] be disentangled from nonsensitive information,” or whether any “protective procedure can salvage” Plaintiffs’ suit. *Kasza*, 133 F.3d 1159, 1166, 1170 (quoting *Ellsberg*, 709 F.2d at 57)).

**D. No Common Law Doctrine Could Override The Court’s Responsibility to Consider a Case of Massive Dragnet Surveillance.**

Absent from both the Government’s and AT&T’s briefs is any acknowledgment of the sheer breadth of their position. They are confronting allegations of the single largest warrantless surveillance program in the history of the Republic. If the evidence Plaintiffs have presented and the information members of Congress have attested to is accurate—and there is little reason to believe otherwise—the Government intercepted communications and received communications records of millions and millions of Americans, without suspicion, much less probable cause. In the face of this massive Fourth Amendment violation, the Government contends that the case must end before it starts—that this Court is powerless even to let the litigation run long enough to see whether Plaintiffs can prove their allegations without jeopardizing national security.

Our forefathers fought a Revolution in protest of abuses like “general warrants” and “writs of assistance.” *Berger v. New York*, 388 U.S. 41, 58-59 (1967) (citing *Entick v. Carrington*, 19 How. St. Tr. 1029 (1765)). Indiscriminate,

general searches—like the searches accomplished by AT&T’s use of its splitter cable to intercept all communications passing through it—are anathema to the Fourth Amendment. *Id.*, 388 U.S. at 59 (holding unlawful “a roving commission to ‘seize’ any and all conversations” with electronic devices because it amounts to a general warrant). The harm to Plaintiffs’ Fourth Amendment rights “is fully accomplished by the original search without probable cause.” *United States v. Calandra*, 414 U.S. 338, 354 (1974).

The Fourth Amendment gives the courts the responsibility to oversee Executive searches through the review and issuance of warrants and through the enforcement of judicial remedies against unconstitutional searches. If credible evidence exists that the Government is using AT&T to engage in dragnet surveillance, capturing the communications of millions of Americans without the pretense of probable cause or reasonable suspicion, the Government cannot do away with the case at its threshold simply by asserting that the very subject matter of the lawsuit—suspicionless general searches systematically conducted on a massive scale over many years without any judicial authorization—is a “state secret.” *See Reynolds*, 345 U.S. at 9-10 (“Judicial control over the evidence in a case cannot be abdicated to the caprice of executive officers.”); *accord, Webster v. Doe*, 486 U.S. 592 (1988) (a “‘serious constitutional question’ . . . would arise if a

federal statute were construed to deny any judicial forum for a colorable constitutional claim”) (citation omitted).

“The basic purpose” of the Fourth Amendment “is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials.” *Camara v. Municipal Ct.*, 387 U.S. 523, 528 (1967). The courts’ constitutional role of policing the Executive under the Fourth Amendment would itself be at risk were the Government correct that it could shield an ongoing, systematic program of dragnet surveillance from any judicial review as a “state secret,” even though substantial evidence of the dragnet exists. This constitutional plan of separated powers gives the Courts a vital role in the protection of constitutional liberties even in times of war.<sup>9</sup> No case has ever suggested that the Fourth Amendment could be

---

<sup>9</sup> See *Hamdi v. Rumsfeld*, 542 U.S. 507, 536 (2004) (plurality) (“Whatever power the United States Constitution envisions for the Executive in its exchanges with other nations or with enemy organizations in times of conflict, it most assuredly envisions a role for all three branches when individual liberties are at stake.”); see also *id.* at 553-54 (Souter, J., concurring in part); see also *id.* at 576 (Scalia, J., dissenting).; cf. *Ex Parte Milligan*, 71 U.S. 2, 120-21 (1866) (“The Constitution of the United States is a law for rulers and people, equally in war and in peace, and covers with the shield of its protection all classes of men, at all times, and under all circumstances.”); cf. *Hamdan v. Rumsfeld*, 126 S.Ct. 2749, 2774 n.23 (2006) (“Whether or not the President has independent power, absent congressional authorization . . . he may not disregard limitations that Congress has, in proper exercise of its own war powers, placed on his powers.”) (citing *Youngstown*, 343 U.S. at 637).

so easily eviscerated—and certainly not on the basis of a common law evidentiary privilege.

**III. LOOKING BEYOND THIS APPEAL, LITIGATING THIS CASE AS CONGRESS INTENDED WILL NOT REQUIRE DISCOVERY OF STATE SECRETS, GIVEN THE LIMITED NATURE OF THE EVIDENCE NECESSARY TO PROVE PLAINTIFFS' CLAIMS AND THE LIMITED NATURE OF AT&T'S POSSIBLE DEFENSES.**

Most of the Government's and AT&T's arguments are not directed at proving that the *entire subject matter* of this suit is a state secret, even though the Government cannot secure a dismissal at the pleading stage without making that showing. *Supra* pp. 19-23. Instead, they spend the bulk of their argument predicting that Plaintiffs will not win their case without secret information that the Government will succeed in withholding (while ignoring FISA's discovery and review protocols) and that AT&T will not be able to proffer evidence necessary to effectively assert a defense. Gov. 26-46; AT&T 22-33, 49-59. Even if they were properly before this Court, those arguments are misplaced.

As a preliminary matter, these speculative arguments are not the proper subject of review by this Court. The District Court recognized that it was premature to reach the issue whether Plaintiffs would be able to prove their prima facie case, or whether AT&T would be unable to present a defense, if in the future the Government invokes the state secrets privilege with respect to specific evidence. *Hepting*, 439 F. Supp. 2d at 994. The District Court declined to decide

these issues in order to allow the case “to proceed to discovery sufficiently to assess the state secrets privilege in light of the facts.” *Id.*<sup>10</sup>

It is manifestly not Plaintiffs’ burden to make their *prima facie* case at this extremely early stage. Additionally, this Court need not find that Plaintiffs have made their case in order to affirm the District Court’s decision. Moreover, Congress has provided a protocol to allow courts to review whatever evidence necessary to determine the legality of the surveillance. Nevertheless, Plaintiffs have already shown that they can make their case without discovery of state secrets. Tellingly, neither the Government nor AT&T identifies a single element of any of the statutory claims that Plaintiffs cannot satisfy with the evidence already adduced.

As demonstrated immediately below, evidence already in the record strongly supports Plaintiffs’ claims, underscoring the impropriety of dismissing the case at its outset. Further, the evidence severely undermines any suggestion that AT&T cannot defend itself without using state secrets.

---

<sup>10</sup> Because the District Court never reached the question whether Plaintiffs can make their *prima facie* case, this Court could decline to consider the question for lack of jurisdiction. *See, e.g., United States v. Stanley*, 483 U.S. 669, 677 (1987) (on a section 1292(b) appeal, “the scope of the issues open to the court of appeals is closely limited to the order appealed from”) (internal quotation marks and citation omitted); *Yamaha Motor Corp. v. Calhoun*, 516 U.S. 199, 205 (1996) (“The court of appeals may not reach beyond the certified order” and may address only those “issue[s] fairly included within the certified order.”).

## **A. Plaintiffs Will Be Able To Prove Their Claims**

The elements of Plaintiffs' statutory claims are straightforward, and the evidence required to establish those claims is minimal. It is simple to illustrate how and why the facts already in the record meet those elements without resort to state secrets. For this Court's convenience, Plaintiffs have set out all the elements of several of their claims in chart form in Appendix A, citing the corresponding evidentiary support for each element.

The basic gist of each statutory provision is the same: Each requires little more than proof that AT&T illegally *intercepted* or *acquired* communications content or that it illegally *disclosed* or *divulged* communications contents or other information pertaining to its customers' communications:

- AT&T violated FISA if it either “(1) engage[d] in electronic surveillance under color of law except as authorized by statute; or (2) disclose[d] . . . information obtained under color of law by electronic surveillance.” 50 U.S.C. § 1809(a).
- AT&T violated one provision of Title III, if it “intentionally intercept[ed] . . . any wire, oral, or electronic communication.” 18 U.S.C. § 2511(1)(a).
- AT&T violated another provision of Title III if it “intentionally disclose[d] . . . 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.” 18 U.S.C. § 2511(1)(c).
- AT&T violated a third provision of Title III if, in the course of “providing an electronic communication service to the public” it “intentionally divulge[d] the contents of any communication . . . while in transmission on that service to any person or entity other than an addressee or intended recipient.” 18 U.S.C. § 2511(3)(a).

- AT&T also violated the Stored Communications Act if it “knowingly divulge[d] a record or other information pertaining to a subscriber to or customer of [its] service (not including the contents of communications . . . ) to any Governmental entity.” 18 U.S.C. § 2702(a)(3).

As the District Court correctly recognized, Plaintiffs’ claims do not rely at all on facts concerning the Government’s handling or use of information that is intercepted or disclosed by AT&T. *Hepting*, 439 F. Supp. 2d at 999. Plaintiffs need not (and do not seek to) allege or prove whether or how the Government analyzed, reviewed, “mined,” or targeted any of that information—only that AT&T acquired it for and disclosed it to the Government. For example:

- To establish an “interception” under Title III, Plaintiffs must show only that the contents of the communication be acquired by a device, not that a human ever review the content. *See* 18 U.S.C. § 2510(4) (defining “intercept” as the “aural or other acquisition” of the “contents” of a “communication” by a “device”); *In re State Police Litigation*, 888 F. Supp. 1235, 1264 (D. Conn. 1995) (“[I]t is the act of diverting, and not the act of listening, that constitutes an ‘interception.’”) (also collecting cases with the same holding).
- To establish “electronic surveillance” under FISA, Plaintiffs again are to focus on the “acquisition” of the “contents” of a “communication” by a “device.” *See* 50 U.S.C. § 1801(f)(2). Those claims do not turn on whether or how the contents were analyzed or reviewed after being acquired. Plaintiffs need not show that their communications have been specifically targeted for surveillance, nor whether or how their contents were analyzed or reviewed after acquisition.
- The statutory prohibitions against illegally “disclos[ing]” or “divulge[ing]” intercepted communications and records to the Government do not require information about whether or how the Government used that information after the disclosure or divulgence.

Plaintiffs’ Fourth Amendment claims are likewise established by evidence of the untargeted, suspicionless, wholesale searches and seizures of the

communications of millions of law-abiding Americans. Plaintiffs do not require any sensitive information about whether or how NSA analysts decide which of the millions of communications and records provided by AT&T are reviewed. Rather, they need only show AT&T's initial acquisition and disclosure to the Government, something they have already established by unrebutted record evidence. Given the Government's use of powers that amount to general warrants or writs of assistance to seize data from millions of Americans, it is of no moment whether it asserts that it has chosen to read or listen to only a "narrowly targeted" subset of the mass of communications caught in AT&T's dragnet (ostensibly those to and from al Qaeda enemy agents). The "special needs" or "inherent authority to . . . surveil[] . . . foreign powers" exceptions to the warrant requirement, which the Government advances only in support of narrowly targeted surveillance of foreign powers, Gov. 37-42, have no bearing on the Fourth Amendment violations actually alleged in the complaint. Those claims do not depend on what the Government did with the communications it seized, but on the bald mass seizures themselves.<sup>11</sup>

---

<sup>11</sup> The Government's similar suggestion that FISA might be unconstitutional where applied to narrowly targeted surveillance of foreign powers, but that answering this question would require discovery of state secrets, is equally off the mark. Gov. 41-43. The Government does not suggest, nor could it, that it could challenge the constitutionality of a statute constraining the dragnet surveillance Plaintiffs challenge. Plaintiffs can prove their claims against the dragnet surveillance they *are* challenging without implicating state secrets. Whether a program in which AT&T exclusively intercepted and disclosed al Qaeda

*(Footnote continued)*

Even if other constitutional claims could be subject to dismissal at the very outset of the case based on the state secrets privilege, the Fourth Amendment claims presented here could not be. To establish their Fourth Amendment claim, Plaintiffs can prove AT&T intercepted virtually all communications headed into and out of the WorldNet Internet room at Folsom Street. And they can prove that AT&T divulged every single one of these communications to the NSA. These facts establish a violation of the Fourth Amendment's per se prohibition on general searches. *See Andresen v. Maryland*, 427 U.S. 463, 480-82 (1976); *Stanford v. Texas*, 379 U.S. 476, 481-84 (1965); *Marcus v. Search Warrant of Prop.*, 367 U.S. 717, 726, 728-29 (1961); *Go-Bart Importing Co. v. United States*, 282 U.S. 344, 357 (1931).

Neither the Government nor AT&T contests that a reasonable factfinder could draw these conclusions from the evidence presented. When the time comes, AT&T is free to argue, if it truly has a basis to do so, that the evidence presented proves no such thing, that there is some benign explanation, that AT&T was not, in fact, involved in any collaboration with the NSA, or that Messrs. Klein and Marcus "don't know anything." AT&T 50 (quoting GER 189). But none of these

---

communications might be constitutional is not an issue in this case. *See ACLU v. NSA*, 438 F. Supp. 2d 754 (E.D. Mich. 2006) (finding such a program unconstitutional).

potential factual assertions could change the fact that Plaintiffs have already produced substantial evidence in support of their claims.

**B. AT&T Will Have a Fair Opportunity to Defend Itself.**

AT&T complains that the Government's invocation of the state secrets privilege will prevent AT&T from fairly defending itself. AT&T 33; 51-52.

Because AT&T never made this argument to the District Court, this Court is free to ignore the argument. *See Connecticut Gen. Life Ins. Co. v. New Images of Beverly Hills*, 321 F.3d 878, 882-883 (9th Cir. 2003). But the argument is meritless, in any event.

As AT&T acknowledges, this basis for dismissal is available only when there is “*no hope of a complete record and adversarial development of the issue[s]*”—*i.e.*, only if the case “*simply could not afford the essential fairness of opportunity to both parties,*” AT&T 28 (quoting *Halkin II*, 690 F.2d at 1000) (emphasis added; other citations omitted). This is not such a case. And as the District Court held, even if it might end up being such a case, there is no way to make that judgment now.

In its effort to overcome this problem, AT&T sounds the familiar refrain that it is not free to confirm or deny the truth of the Klein materials, while ignoring the process set forth in Section 1806(f). AT&T 51-52. That is incorrect. If AT&T wishes to deny, contrary to its own already submitted sworn declaration, that it has

a secret room to which all internet communications have been diverted, or that the NSA has access to the room, it is free to do so, just as numerous telephone companies did in the wake of news reports of massive Government dragnets. No national security interest could possibly be implicated by such a denial—unless it is false. Moreover, AT&T itself has already presented evidence about the Klein materials in support of its claim that they include trade secrets. SER 507-15.

AT&T's argument also fails because the Government has removed any barrier to AT&T's defense. When the Government declared that the contents of the Klein materials are not subject to the state secrets privilege—and that Plaintiffs are free to prove the facts Klein described—it waived any ability to assert that privilege to exclude the facts in those materials. *See supra* pp. 37-39. The Government cannot declare that the contents of AT&T's extensive schematic diagrams and tables are not secret, and that AT&T's former employee's account of how NSA collaborated with AT&T is not secret, but then insist that they are secrets when AT&T itself discusses or contests them.

Under the Federal Rules of Evidence, “the privilege of a . . . *government* . . . shall be governed by the principles of the common law as they may be interpreted by the courts of the United States in the light of reason and experience.” Fed. R. Evid. 501 (emphasis added). One of those “principles of the common law” is that voluntary disclosure of the content of privileged information “constitutes waiver of

the privilege as to all other such communications on the same subject.” *Weil v. Invest./Indicators, Research & Mgmt.*, 647 F.2d 18, 24 (9th Cir. 1981) (applying subject -matter waiver to attorney-client privilege).

The Government makes much of its contention that AT&T might be able to assert that it had permission from the Government to engage in its interception and disclosure activities, but that AT&T would be barred by the state secrets privilege from asserting the certification as a defense. Gov. 45-46. The District Court was correct in rejecting this contention. *See Hepting*, 439 F. Supp. 2d at 995-97.

AT&T’s putative “certification” defense is based on the following statutory provision:

[P]roviders of wire or electronic communication service . . . are authorized to provide information, facilities, or technical assistance to persons authorized by law to intercept wire, oral, or electronic communications . . . *if such provider . . . has been provided with . . . a certification* in writing by [specified Government officials] or the Attorney General . . . *that all statutory requirements have been met . . . .*

18 U.S.C. § 2511(2)(a)(ii) (emphasis added).

If, in fact, AT&T secured such a certification, and even if that certification would insulate AT&T from liability for years of surveillance (which it would not), AT&T’s argument would be unavailing. The state secrets privilege would not impede AT&T’s ability to raise a certification defense altogether. No such barrier exists for two reasons.

First, the specific statutory provisions relating to such certifications eliminate the barrier. Where a certification complies with the necessary formalities and is properly obtained, the express statutory purpose for providing the certification to a private party like AT&T is to shield it from liability. *See* 18 U.S.C. § 2511(2)(a)(ii) (“No cause of action shall lie in any court against any provider . . . for providing information, facilities, or assistance in accordance with the terms of a . . . certification.”). This defense would be completely illusory if a common law privilege, at the same time, prohibited any disclosure in litigation of certifications on which the private party had relied. Congress did not create an illusory defense. Section 2511(2)(a)(ii) explicitly provides for the disclosure by a private party of a certification “as may otherwise be required by legal process” after notifying the Attorney General.

Second, the discovery and review protocols of Section 1806(f) also give AT&T a procedure by which to assert a certification defense if one exists. Those provisions dovetail with the notice requirements of Section 2511(2)(a)(ii)—upon notification, the Attorney General may invoke the procedures of Section 1806(f) if he or she is concerned that the disclosure of the certification may harm national security. A certification falls within the scope of the protocol because it would be “material[] relating to the surveillance” “necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted.” 50

U.S.C. § 1806(f). Just as a court may examine a court order authorizing surveillance to assess the legality of the surveillance it purportedly authorizes, so, too, does Section 1806(f) permit the court to examine any certification by the Attorney General that purportedly authorizes the surveillance of the sort alleged here.

The District Court thus correctly concluded that the possibility of certification defense is no bar to proceeding.

#### **IV. THE DISTRICT COURT CORRECTLY DENIED THE MOTIONS TO DISMISS THE COMPLAINT ON STANDING GROUNDS.**

Plaintiffs have pled that AT&T has diverted their personal communications and records to the NSA. Even without discovery, they have already proved that point to a near certainty. Nevertheless, in an argument propounded mainly by AT&T, AT&T and the Government contend that Plaintiffs lack standing—and specifically that they have not sufficiently pled or proven injury in fact.<sup>12</sup> They are wrong.

---

<sup>12</sup> To demonstrate standing Plaintiffs need only plead enough facts to satisfy three elements: (1) “injury in fact,” (2) “a causal connection between the injury and the conduct complained of”; and (3) that it is “likely . . . that the injury will be redressed by a favorable decision.” *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560-61 (1992) (internal quotations and citations omitted). AT&T couches in “standing” terms—under the latter two elements—several of its arguments about whether Plaintiffs will be able to prove their case. These arguments are addressed earlier in this brief.

AT&T's position begins with an incorrect account of Plaintiffs' allegations. *See infra* Point IV.A. Much of AT&T's analysis is built around the incorrect supposition that Plaintiffs must *prove* their standing at this early stage of the litigation. *See infra* Point IV.B. AT&T also incorrectly predicts that no Plaintiff will ever be able to prove for certain—without seeking secret information—that his or her own communications were intercepted. AT&T is wrong both about whether Plaintiffs need to prove any such thing, and about whether they can prove it. Plaintiffs have already proven the fact to a near certainty for their key claims. *See infra* Point IV.C. Pursuant to the protocols Congress set forth in Section 1806(f), the court is entitled to review any additional material it believes appropriate to determine the legality of the surveillance, and, even without secret information, Plaintiffs will be able to prove it even more fully as the case progresses. *See infra* Point IV.D. Largely for these reasons, the few cases AT&T invokes for its standing argument are distinguishable. *See infra* Point IV.E.

**A. Plaintiffs' Allegations Defeat a Motion to Dismiss at the Pleading Stage.**

The facts Plaintiffs allege, which must be taken as true on a motion to dismiss, are straightforward: the named Plaintiffs all were, and some still are, AT&T customers. GER 4. Two of them allege that they were, or still are, WorldNet subscribers and users. GER 4, 10-13. As we have seen, Plaintiffs allege a massive dragnet that diverts to the NSA the “content of all or a substantial

number of wire communications transferred through the AT&T Corp. facilities.”

GER 9. Critically, the complaint also explicitly alleges, several times, that the AT&T dragnet intercepted each Plaintiff’s own personal communications and records. GER 9-10, 12, 19, 21-26, 28. The complaint accuses AT&T, for example, of “intercepting and disclosing to the government the contents of its customers’ communications as well as detailed communications records about millions of its customers, *including Plaintiffs and class members.*” GER 3 (emphasis added). Similarly, Plaintiffs allege that “AT&T Corp. used or assisted in the use of . . . devices to acquire wire or electronic communications *to which Plaintiffs and class members were a party*, and to acquire [records] information pertaining to those communications.” GER 10 (emphasis added).

Plaintiffs also allege that the dragnet is ongoing—“Defendants continue to do so,” GER 10—which is why they seek an injunction. GER 30. While the Government now purports to have sought and obtained FISA court authorization for its targeted surveillance of al Qaeda suspects, Gov. 9-10, the Government has never suggested that it has secured or even sought such authorization for the dragnet surveillance at issue in this case. *See* Gov. 33-34.

These allegations are more than enough to satisfy injury in fact. Let us put aside for a moment the injury from future surveillance and focus, as AT&T does, just on past harm. AT&T does not dispute that Plaintiffs could establish injury in

fact, at least in an ordinary case, with a simple allegation that that AT&T intercepted and diverted “the contents or records of *their* communications.” AT&T 44. As the D.C. Circuit has held, allegations of the “interception of plaintiffs’ private communications” are allegations “which if proved would constitute an injury in fact, permitting plaintiffs to go forward in an effort to prove the truth of those allegations.” *Halkin II*, 690 F.2d at 999. The District Court was correct when it observed that “the alleged injury is concrete even though it is widely shared.” *Hepting*, 439 F. Supp. 2d at 1001; *see FEC v. Akins*, 524 U.S. 11, 24 (1998).

In arguing that the ordinary rule does not apply here, AT&T asserts that “[t]he relevant paragraphs [of the complaint] are hedged and do not allege that this program entailed the surveillance of *all* communications of *every* AT&T customer or subscriber.” AT&T 47 (emphasis added). But to plead injury for standing purposes, Plaintiffs need not allege that *every single* communication of *every single* AT&T customer was diverted to the NSA. It is, therefore, irrelevant that the complaint has a passage (the only one AT&T cites in support of the proposition that *all* “the relevant paragraphs” in the complaint “are hedged”) that says AT&T is diverting the “content of all *or a substantial number* of the wire or electronic communications transferred through the AT&T Corp. facilities.” AT&T 47 (quoting GER 9; emphasis added by AT&T). It is more than enough for Plaintiffs

to allege—as they have in the passages quoted above and numerous others—that they each suffered a diversion of at least one such communication. (Plaintiffs contend that is *more* than enough, because Plaintiffs were not required to allege—and need not eventually prove—even that much. *See infra* pp. 75-80.) That is exactly what Plaintiffs intend to prove, and they are entitled to an opportunity to do so. *See Halkin II*, 690 F.2d at 999 (dismissing the case, on summary judgment, only after plaintiffs were unable to prove what they set out to prove, without revealing state secrets).

For these reasons, AT&T is wrong to argue that standing has not been adequately pled as to *past* violations. But AT&T’s argument is all the more flawed, because it is inapplicable to *future* violations. As demonstrated below, even a significant possibility of future interceptions will suffice to establish standing—and there is no doubt Plaintiffs alleged at least that.

**B. Plaintiffs Are Not Required to *Prove* Standing at this Early Stage.**

AT&T filed a motion to dismiss on standing grounds, not a motion for summary judgment. Thus, Plaintiffs were not required to oppose AT&T’s motion with the definitive *proof* by which they intend to demonstrate their standing. Elements of standing, like all other elements of a plaintiff’s case, need only be “supported . . . with the manner and degree of evidence required at the successive stages of the litigation.” *Lujan*, 504 U.S. at 561; *see Steel Co. v. Citizens for a*

*Better Env't*, 523 U.S. 83, 104 (1998) (holding that on a motion to dismiss, plaintiffs need only show that facts alleged, if proved, would confer standing). In light of this procedural posture, the Government's and AT&T's repeated assertions that Plaintiffs must now "prove" their standing at this early stage of the case are mystifying. *E.g.*, Gov. 26; AT&T 23, 49.

The rule does not change just because the Government filed a motion to dismiss that was couched in the alternative as a summary judgment motion on the state secrets privilege. Plaintiffs filed a statement under Rule 56(f) specifying the discovery they should be permitted to conduct before having to respond to a motion for summary judgment—including facts relating to standing.<sup>13</sup> *See* Fed. R. Civ. P. 56(f); SER 587-92. On that basis, the District Court had the discretion to treat the motion for summary judgment on standing grounds as a motion to dismiss. *See, e.g., National Coal. for Students with Disabilities Educ. and Legal Defense Fund v. Scales*, 150 F. Supp. 2d 845, 848 (D. Md. 2001). That is exactly what the District Court did. *See Hepting*, 439 F. Supp. 2d at 1001.

Nor do the ordinary rules of pleading and proof change just because the Government is invoking the state secrets privilege. AT&T's assertion at the pleading stage that "the state secrets privilege will prevent Plaintiffs from *proving*

---

<sup>13</sup> As discussed above, the parties are entitled to take further discovery as necessary, subject to the provisions set forth in Section 1806(f).

any such allegations,” AT&T 48 (emphasis AT&T’s), does not entitle AT&T to demand the relevant proof now. *See Halkin II*, 690 F.2d at 999. And even if the state secrets privilege entitled AT&T to a preview of what Plaintiffs might offer on summary judgment after discovery, it certainly does not entitle them to insist that Plaintiffs provide more than “at least some factual basis” for standing, which the District Court found they had done. *Hepting*, 439 F. Supp. 2d at 1001. Contrary to AT&T’s assertion, that *is* “the relevant test” at the summary judgment phase, and AT&T cannot contort the usual rules to insist that “Plaintiffs bear the burden of *establishing* standing,” at this early stage. AT&T 49 (emphasis AT&T’s). Not until trial will Plaintiffs be expected to “*prove* that untargeted dragnet surveillance . . . actually occurred” or “that any such surveillance captured Plaintiffs’ communications.” AT&T 49-50 (emphasis added). Even if this case were treated as though it were an appeal from the denial of a summary judgment motion—contrary to the District Court’s intention and to the motion AT&T actually filed—“plaintiffs need not establish that they in fact have standing, but only that there is a genuine question of material fact as to the standing elements.” *See Central Delta Water Agency v. United States*, 306 F.3d 938, 947 (9th Cir. 2002) (at summary judgment).

When the appropriate time comes—at trial—AT&T is free to challenge any “assumptions” or “speculation” in which it believes Mr. Marcus indulged. AT&T

50. AT&T is also free to argue that testimony by Mr. Klein and Mr. Marcus “are not evidence from those ‘indisputably situated to disclose’ reliable information,” AT&T 50, or to challenge Mr. Klein on cross-examination as to “whether a secure room really existed, what its purpose was, what information (if any) went into the supposed room,” and the wide variety of other factual questions AT&T poses. AT&T 51. But for now, the evidence—which is both sworn, undisputed and on some points confirmed by AT&T’s declaration—is enough to present at least an issue of fact for trial as to Plaintiffs’ standing.

**C. The Evidence Plaintiffs Have Already Adduced Is Sufficient to Satisfy Standing.**

AT&T’s main point is that Plaintiffs must *now* demonstrate that they *will* be able to prove injury in fact without resort to state secrets. Plaintiffs have no such burden now, but even if they did, they can satisfy it. Indeed, they already have.

**1. The evidence already adduced establishes that AT&T diverts all, or substantially all, of the peered internet traffic in the area.**

Already, without resort to state secrets (and without any discovery), Plaintiffs have presented enough evidence to satisfy standing—even for summary judgment purposes. One need look no further than telecommunications expert Scott Marcus’s non-privileged expert testimony. Contrary to AT&T’s assertion, that testimony does not “depend[] entirely,” nor even primarily, “on the Klein declaration,” AT&T 53, which is, in any event, unrebutted. Rather, it is based

largely on a painstaking analysis of AT&T's own schematics and tables of data. It was on that basis that the expert concluded that "the traffic that was diverted represented *all, or substantially all*, of AT&T's peering traffic in the San Francisco Bay Area." SER 164 (emphasis added); SER 146-47.

According to Mr. Marcus, for AT&T customers in the San Francisco area, peered communications "would have been handed off to peers at the first available opportunity . . . and thus would with high probability have been handed off through the Folsom Street facility." SER 165. Further, the expert concludes that "more than half of all Internet traffic was likely intercepted (at least, at a physical level) for *all* AT&T customers," not just those who live in California. SER 170. "A fiber splitter, in its nature, is not a selective device—*all* the traffic on the split circuit was diverted or copied." SER 166 (emphasis added).

While these passages are couched in the past tense, neither the Government nor AT&T has offered any reason to believe that the illegal interceptions and diversions described by Plaintiffs' expert have stopped.

**2. The evidence establishes standing both to sue over past interceptions and to enjoin future ones.**

AT&T asserts that this is not enough, because "[i]n order to establish injury-in-fact, Plaintiffs must demonstrate that the content or records of *their* communications *were* intercepted by the NSA." AT&T 44 (first emphasis in

original) (second emphasis added). AT&T's objection is misplaced for two reasons.

First, the evidence already adduced *does* establish exactly that. Granted, Mr. Marcus did not swear that AT&T diverted literally *all* of its peering traffic in San Francisco. No credible expert would make such a categorical statement. Rather, he said, "the traffic that was diverted represented *all, or substantially all*, of AT&T's peering traffic in the San Francisco Bay Area." SER 164 (emphasis added). That means that if any particular Plaintiff sent or received only a single peered internet communication there was an overwhelming likelihood that AT&T intercepted it and diverted it to the NSA. But this case is not about one email. Plaintiffs allege they have been regular AT&T subscribers and users over the course of many years. GER 4. They further allege that the surveillance has continued for many years. GER 8. For a normal customer, who sends and receives thousands of internet communications or phone calls over the course of several years, it is inconceivable that at least one of her communications would not have been intercepted.

Second, no such certainty is necessary to establish standing. Plaintiffs can establish injury in fact by proving either the *likelihood* that their *past* communications were intercepted or the *likelihood* that their *future* communications will be intercepted. As to the future, "[t]he courts of appeals have

generally recognized that threatened harm in the form of an increased risk of future injury may serve as injury-in-fact for Article III standing purposes.” *Baur v. Veneman*, 352 F.3d 625, 633 (2d Cir. 2003) (holding plaintiff had standing to challenge USDA regulations that increased likelihood that beef carrying “mad cow disease” could be sold, based on an allegation that the plaintiff ate meat regularly).<sup>14</sup> As to the past, the courts have also consistently allowed plaintiffs to sue based upon past events, even where they cannot prove with certainty that they personally suffered the injury.<sup>15</sup> As this Court has observed “even a *small*

---

<sup>14</sup> See, e.g., *Helling v. McKinney*, 509 U.S. 25, 35 (1993) (concluding that a prisoner could bring an Eighth Amendment claim based on allegations that prison officials had “exposed him to levels of [second-hand smoke] that pose an unreasonable risk of serious damage to his future health”); *American Library Ass’n v. FCC*, 401 F.3d 489, 493 (D.C. Cir. 2005) (holding that where librarians’ association sought review of an FCC rule, injury-in-fact could be established by showing “that there is a substantial probability that the FCC’s order will harm the concrete and particularized interests of at least one of their members”); *Hall v. Norton*, 266 F.3d 969, 976 (9th Cir. 2001) (plaintiff had standing to challenge government’s exchange of land with private developer under Clean Air Act based on allegation that new development could aggravate his respiratory discomfort).

<sup>15</sup> See, e.g., *Clinton v. New York*, 524 U.S. 417, 432 (1998) (New York had standing to challenge line item veto law where President vetoed provision that New York could have used as a “statutory ‘bargaining chip,’” based on reasoning that “the cancellation inflicted a sufficient likelihood of economic injury to establish standing under our precedents”); *Covington v. Jefferson County*, 358 F.3d 626, 641 (9th Cir. 2004) (holding that evidence of leakage of ozone-depleting materials was “sufficient to show injury in fact because the failure to comply with [the Clean Air Act] has increased the risk of harm to the Covingtons’ property”); *Baur*, 352 F.3d at 641 (“[A]s we have clarified, the relevant ‘injury’ for standing

(Footnote continued)

*probability of injury is sufficient to create a case or controversy.” Central Delta Water Agency v. United States, 306 F.3d 938, 949 (9th Cir. 2002) (citation and internal quotations omitted; emphasis added). Certain harms are “‘by nature probabilistic,’ yet an unreasonable exposure to risk may itself cause cognizable injury.” Baur, 352 F.3d at 634 (quoting Friends of the Earth, Inc. v. Gaston Copper Recycling Corp., 204 F.3d 149, 160 (4th Cir. 2000)).*

In keeping with this principle, the Supreme Court and the Courts of Appeals have repeatedly found that a plaintiff satisfies standing by alleging (or demonstrating) that conditions “pose an *unreasonable risk* of serious . . . damage,” *Helling*, 509 U.S. at 35 (emphasis added), or that legislation “inflicted a *sufficient likelihood* of economic injury,” *Clinton*, 524 U.S. at 432 (emphasis added), or even that “[t]he probability [of a financial consequence] *does not seem negligible*, though no stronger statement is possible.” *United States v. Pawlinski*, 374 F.3d 536, 539 (7th Cir. 2004) (emphasis added). The overwhelming probability of harm already confirmed by the evidence in this case easily meets any of these standards.

This Court’s decision in *LaDuke v. Nelson* is especially instructive on this point. 762 F.2d 1318, 1322-26 (9th Cir. 1985). There, as here, a class of plaintiffs sued the government for illegal searches. A class of migrant farm workers sued the

---

purposes may be exposure to a sufficiently serious risk of medical harm—not the anticipated medical harm itself.”)

INS to enjoin a pattern of warrantless searches of migrant farm dwellings within a large, three-state region. *Id.* at 1321. The INS had obviously not searched every single migrant home within those three states, and no individual plaintiff could establish with certainty that his dwelling would be subjected to one of the INS's warrantless searches in the future. *Id.* at 1322-26. Nonetheless, this Court held that the plaintiff class had standing, based on nothing more than a district court finding that such searches would likely recur within the three-state region in which the plaintiffs resided at some (indefinite) point in the future. *Id.* at 1322-26. If that likelihood of future government intrusion sufficed in *LaDuke*, than the virtual certainty of past interceptions and the extreme likelihood of future interceptions here should suffice as well.

**D. Any Further Evidence Plaintiffs Might Need to Establish Standing Can Be Gathered Without Divulging State Secrets.**

Even if individual Plaintiffs were required eventually to prove with absolute certainty that their personal communications were in fact intercepted or disclosed, or are currently being intercepted, they could do so without seeking state secrets. For the interception claims, as demonstrated more fully above, any communication that reaches the splitter cable is necessarily diverted to the NSA. *See supra* 60-64; *infra* Appendix A. In order to prove that AT&T diverted one of Plaintiffs' communications, then, all Plaintiffs have to prove is that their communication reached the splitter cable.

That is a simple matter. Plaintiffs merely have to trace a message from each Plaintiff's home machine and record each stop it makes along the journey to its final destination. To do that, a trained technician need never step foot on AT&T's property, much less enter AT&T's secret room. Plaintiffs do not have to prove anything about what the NSA did with the communication once the communication entered the secret room. And they certainly do not have to prove "what [the secret room's] purpose was, . . . what equipment was in the room, [or] what happened to any such information inside the room." AT&T 51. As for communication record claims, Plaintiffs need only demonstrate that AT&T's massive database of communications records, which is not in any way a secret, includes at least some of their records—something that must be the case if AT&T is properly billing them for the communication services they receive. *See supra* pp. 45-55, 60-64.

To the extent that the court finds it needs additional information to determine the legality of the surveillance and the Government asserts that disclosure of such information would harm national security, the procedures of Section 1806(f) provide for the requisite discovery without undue risk of disclosure.

**E. The Decisions AT&T Invokes Do Not Justify Dismissal of a Dragnet Case Involving Dragnet Surveillance on the Pleadings.**

In support of its argument that dismissal for lack of standing is appropriate here at the pleading stage, AT&T cites some of the same cases discussed above in the context of the broader discussion over the application of the state secrets privilege—the two *Halkin* cases and *Ellsberg*. *See supra* pp. 53-55. These cases are equally inapposite in the standing context, and for some of the same reasons.

First and foremost, none of these cases entailed dismissal on standing grounds *at the inception*. They all involved dismissals after extensive discovery. *See Halkin II*, 690 F.2d at 985; *Ellsberg*, 709 F.2d at 53-56.

Second, none of these cases stands for the proposition that a case like this— involving *dragnet* surveillance—must be dismissed for failure to prove that a specific communication by a specific plaintiff had been intercepted. Rather, those cases focused on *targeted* surveillance programs, more akin to the TSP’s targeting of international communications by those with links to al Qaeda, conduct that is not at issue in this case.

The *Halkin* cases illustrate the distinction. *Halkin I*’s analysis of the state secrets privilege focused almost entirely on an NSA surveillance operation (called MINARET) that selected messages to, from, or mentioning specifically targeted individuals and organizations who were on a “watchlist” from out of a larger group of the messages the NSA acquired by monitoring certain specifically targeted

international communications circuits. *Halkin I*, 598 F.2d at 4, 11 & n.8; *see also Halkin II*, 690 F.2d at 983 & n.23; Church Committee, Book III at 743-44, 748-49. The court upheld the privilege because “confirmation or denial of acquisition of a *particular individual’s* international communications” could “provide valuable information as to what circuits were monitored and what methods of acquisition were employed,” and “would enable foreign governments or organizations to extrapolate the focus and concerns of our nation’s intelligence operations.” *Halkin I*, 598 F.2d at 8. On the basis of this reasoning, the court found that “the identification of the individuals or organizations whose communications have or have not been acquired presents a reasonable danger that state secrets would be revealed.” *Id.* at 9.<sup>16</sup>

*Halkin II* reached a similar conclusion on a variation of the same facts. By that point in the litigation, after further discovery and pretrial proceedings, the

---

<sup>16</sup> *Halkin I* also involved a broader program, code-named SHAMROCK. *Halkin I*, 598 F.2d at 4. Because all acquisitions, for both the targeted program and the broader program, were processed identically, the court stated—without further analysis—that “our reasoning [regarding the NSA’s state secrets claim] applies to both” programs. *Id.* at 10. Thus, the court was evidently concerned that confirming or denying particular interceptions from either program would necessarily reveal secret information about the subsequent processing. *See id.* at 6 (processing consisted of the NSA’s compilation of watchlists of names supplied by the FBI, CIA and various other agencies, and the NSA’s provision of edited or summarized versions of communications to, from, or containing these names to the requesting agencies).

plaintiffs' only remaining claim was a targeted surveillance claim against defendants who allegedly indirectly caused targeted surveillance to occur, but did not participate in the surveillance themselves. The plaintiffs alleged that "the CIA and the individuals responsible for submitting the watchlists to the NSA could be held liable based on a presumption that the submission of a name resulted in interception of the named person's communications." *Halkin II*, 690 F.2d at 984 (emphasis added). But they had no proof that the NSA actually did any such thing. In particular, this was true because the NSA used the watchlist to select messages mentioning a person who was not a party to the communication (*e.g.*, a message on a circuit "used by the North Vietnamese to communicate with their representatives in Paris and other places" regarding "[r]eports of meetings with American and anti-war groups," *Halkin I*, 598 F.2d at 11 n.8), and thus the presence of a name on the watchlist did not suggest that that person's communications were being monitored. *Halkin I*, 598 F.2d at 11 & n.8; *Halkin II*, 690 F.2d at 983 & n.23. The Court of Appeals thus affirmed the district court's holding that "plaintiffs cannot show any injury from having their names submitted to NSA because NSA is prohibited from disclosing whether it acquired any of plaintiffs' communications." *Id.* at 997 (quoting district court opinion). Notably, this dismissal came six years after the case was filed, and only after "the parties [had] fought the bulk of their dispute on

the battlefield of discovery” regarding the propriety of *specific* discovery requests. *Id.* at 984.

*Ellsberg* did not purport to be a ruling about standing. Rather, the Court upheld the dismissal of several plaintiffs’ claims based on their inability “to make out a *prima facie* case without [secret] information.” *Ellsberg*, 709 F.2d at 65. In *Ellsberg*, as in the *Halkin* cases, the 16 plaintiffs challenged *targeted* surveillance. *Id.* at 53. In response to interrogatories, the Government conceded that it had intercepted conversations of five of them during foreign intelligence wiretaps. *Id.* at 55. As to the remaining 11, the Government “conceded ‘foreign intelligence’ surveillance of ‘one or more of the plaintiffs,’ thus leaving open the possibility that others in the plaintiff class had been overheard.” *Id.* The Court dismissed these 11 plaintiffs’ claims on the ground that none could prove that the Government had in fact intercepted his calls. *Id.* at 65.

These cases do not compel dismissal here, for all the reasons discussed earlier in this section: (1) this case is just at the pleading stage; (2) this is a dragnet case that does not depend upon secret information about whether any particular Plaintiff was targeted; (3) Plaintiffs have already proven to a near certainty that their communications were intercepted; (4) Plaintiffs can easily prove, without resorting to any state secrets, that their communications and records are headed to a pipeline that leads to the NSA’s secret room; and (5) Congress created private

rights of action and superseded the common law state secrets privilege to allow courts to review purportedly secret material as necessary to adjudicate electronic surveillance cases.

**CONCLUSION**

For the foregoing reasons, this Court should affirm the District Court's denial of the motions to dismiss by the Government and AT&T and its denial of the Government's motion for summary judgment.

DATED: April 26, 2007

ELECTRONIC FRONTIER FOUNDATION

HELLER EHRMAN LLP

By *Cindy A. Cohn* /SE By *Robert D. Fram*

CINDY A. COHN  
LEE TIEN  
KURT OPSAHL  
KEVIN S. BANKSTON  
JAMES S. TYRE  
454 Shotwell Street  
San Francisco, CA 94110  
Telephone: (415) 436-9333 x108  
Facsimile: (415) 436-9993

ROBERT D. FRAM  
E. JOSHUA ROSENKRANZ  
MICHAEL M. MARKMAN  
ETHAN C. GLASS  
SAMUEL F. ERNST  
NATHAN E. SHAFROTH  
ELENA DIMUZIO  
333 Bush Street  
San Francisco, CA 94104  
Telephone: (415) 772-6000  
Facsimile: (415) 772-6268

ATTORNEYS FOR APPELLEES

LAW OFFICE OF RICHARD R. WIEBE  
RICHARD R. WIEBE  
425 California Street  
Suite 2025  
San Francisco, CA 94104  
Telephone: (415) 433-3200  
Facsimile: (415) 433-6382

LERACH COUGHLIN STOIA  
GELLER RUDMAN & ROBBINS LLP  
ERIC ALAN ISAACSON  
655 West Broadway, Suite 1900  
San Diego, CA 92101-3301  
Telephone: (619) 231-1058  
Facsimile: (619) 231-7423

HAGENS BERMAN SOBEL SHAPIRO LLP  
REED R. KATHREIN  
JEFFREY FRIEDMAN  
SHANA E. SCARLETT  
425 Second Street, Suite 500  
San Francisco, CA 94107  
Telephone: (415) 896-6300  
Facsimile: (415) 896-6301

LAW OFFICE OF ARAM ANTARAMIAN  
ARAM ANTARAMIAN  
1714 Blake Street  
Berkeley, CA 94703  
Telephone: (510) 841-2369

**Appendix: Plaintiffs Can Support Each Element  
Of Their Statutory Claims With Non-Privileged Evidence**

Statutory Element	Plaintiffs' Non-privileged Evidence
<b>18 U.S.C. § 2511</b>	
1. AT&T “intentionally . . .”	AT&T trained and paid employees to split and redirect the circuits carrying Plaintiffs’ communications. SER 3.
2. “intercept[ed]” Plaintiffs’ “wire, oral, or electronic communications” (where “intercept” is defined as “aural or other acquisition of the contents of any . . . communication through the use of any electronic . . . or other device.” 18 U.S.C. § 2510(4))	AT&T used a splitter cabinet to duplicate Plaintiffs’ communications and direct them into the SG3 Secure Room. SER 5. Splitting the cable duplicates the information, making a copy of the contents of the communications. SER 5.
3. (and “device” includes “any device which can be used to intercept a wire, oral or electronic communication other than . . . equipment . . . being used by a provider of wire or electronic communication service in the ordinary course of its business.” <i>Id.</i> § 2510(5))	Only employees with NSA security clearance had access to the SG3 Secure Room. SER 4. Persons with NSA security clearance do not act within the ordinary course of business, but rather to perform a governmental function. Exec. Order § 12968 §§ 1.2(a), 1.1(h), 1.1(e).
<b>50 U.S.C. § 1809(a)</b>	
4. AT&T “engage[d] in electronic surveillance . . .” (where “electronic surveillance” means the acquisition by a device of the contents of any wire communication in the United States. 50 U.S.C. § 1801(f))	<i>See</i> rows 2 and 3, <i>supra</i> .
5. “under color of law.”	Only employees with NSA security clearance had access to the SG3 Secure Room. SER 4. Persons with NSA clearance act on behalf of the Government. Exec. Order § 12968 §§ 1.2(a), 1.1(h), 1.1(e).

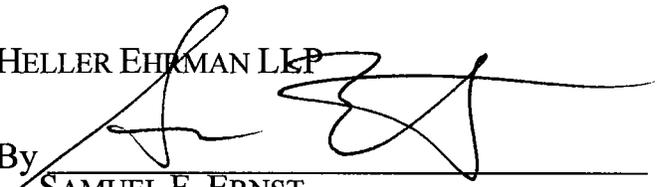
<b>18 U.S.C. § 2511(1)(c)</b>	
6. AT&T “intentionally . . .”	<i>See row 1, supra.</i>
7. “disclose[d] . . . to any other person . . .”	AT&T directed a copy of Plaintiffs’ communications into the SG3 Secure Room. SER 5. This disclosure was to an “other person” because only persons with NSA security clearance could enter the SG3 Secure Room. SER 4. Persons with NSA security clearance were acting as governmental agents. Exec. Order § 12968 §§ 1.2(a), 1.1(h), 1.1(e).
8. “the contents of any wire, oral, or electronic communication . . .”	AT&T provided a copy of the contents of Plaintiffs’ communications to the SG3 Secure Room. SER 5.
9. “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.”	<i>See row 1, supra.</i>
<b>18 U.S.C. § 2511(3)(a)</b>	
10. “[A] person or entity providing an electronic communication service to the public shall not intentionally . . .”	<i>See row 1, supra.</i>
“divulge . . . to any person or entity other than an addressee or intended recipient . . .”	<i>See row 7, supra.</i>
11. “the contents of any communication . . . “	<i>See row 8, supra.</i>
<b>18 U.S.C. § 2702(a)(3)</b>	
12. AT&T, “a provider of remote computing service or electronic communication service to the public[,] shall not knowingly . . .”	<i>See row 1, supra.</i>
13. “divulge . . . to any governmental entity . . .”	<i>See row 7, supra.</i>

14. “a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications . . .) . . . .”	The communications directed by AT&T into the SG3 Secure Room include not only the contents of communications but non-content addressing information. SER 150.
--	---

**CERTIFICATE OF COMPLIANCE**

I certify that this brief uses a proportional typeface and 14-point font, and contains 19,796 words, counted according to Fed. R. App. P. 32(a)(7)(B)(iii). Plaintiffs have filed herewith a motion to file an enlarged brief pursuant to Ninth Circuit Rule 32-2.

DATED: April 26, 2007

HELLER EHRMAN LLP  
By   
SAMUEL F. ERNST

ATTORNEYS FOR APPELLEES

**STATEMENT OF RELATED CASES**

Pursuant to Ninth Circuit Rule 28-2-6, Plaintiffs-Appellees state that they are aware of no other related cases pending in this Court beyond those identified by Appellants.

# **ADDENDUM**

## ADDENDUM TABLE OF CONTENTS

	<b><u>Page</u></b>
50 U.S.C. 1801 .....	1a
50 U.S.C. 1806 .....	2a
50 U.S.C. 1809 .....	3a
50 U.S.C. 1810 .....	3a
50 U.S.C. 2510 .....	4a
18 U.S.C. 2511 .....	8a
18 U.S.C. 2520 .....	15a
18 U.S.C. 2702 .....	17a
18 U.S.C. 2707 .....	19a

**50 U.S.C. 1801**

**§ 1801. Definitions**

\*\*\*\*

**(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.

**(l)** “Wire communication” means any communication while it is being carried by a wire, cable, or other like connection furnished or operated by any person engaged

as a common carrier in providing or operating such facilities for the transmission of interstate or foreign communications.

**(m)** “Person” means any individual, including any officer or employee of the Federal Government, or any group, entity, association, corporation, or foreign power.

**(n)** “Contents”, when used with respect to a communication, includes any information concerning the identity of the parties to such communication or the existence, substance, purport, or meaning of that communication.

\*\*\*\*

## **50 U.S.C. 1806**

### **§ 1806. Use of Information**

\*\*\*\*

**(f)** In camera and ex parte review by district court

Whenever a court or other authority is notified pursuant to subsection (c) or (d) of this section, or whenever a motion is made pursuant to subsection (e) of this section, or whenever any motion or request is made by an aggrieved person pursuant to any other statute or rule of the United States or any State before any court or other authority of the United States or any State to discover or obtain applications or orders or other materials relating to electronic surveillance or to discover, obtain, or suppress evidence or information obtained or derived from electronic surveillance under this chapter, the United States district court or, where the motion is made before another authority, the United States district court in the same district as the authority, shall, notwithstanding any other law, if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States, review in camera and ex parte the application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted. In making this determination, the court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance.

\*\*\*\*

**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.

**b) Defense**

It is a defense to a prosecution under subsection (a) of this section that the defendant was a law enforcement or investigative officer engaged in the course of his official duties and the electronic surveillance was authorized by and conducted pursuant to a search warrant or court order of a court of competent jurisdiction.

**c) Penalties**

An offense described in this section is punishable by a fine of not more than \$10,000 or imprisonment for not more than five years, or both.

**d) Federal jurisdiction**

There is Federal jurisdiction over an offense under this section if the person committing the offense was an officer or employee of the United States at the time the offense was committed.

**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.

### **18 U.S.C. 2510**

#### **§ 2510. Definitions**

As used in this chapter--

**(1)** "wire communication" means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce;

**(2)** "oral communication" means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication;

**(3)** "State" means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any territory or possession of the United States;

**(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.

**(5)** “electronic, mechanical, or other device” means any device or apparatus which can be used to intercept a wire, oral, or electronic communication other than--

(a) any telephone or telegraph instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business; or (ii) being used by a provider of wire or electronic communication service in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties;

(b) a hearing aid or similar device being used to correct subnormal hearing to not better than normal;

**(6)** “person” means any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation;

**(7)** “Investigative or law enforcement officer” means any officer of the United States or of a State or political subdivision thereof, who is empowered by law to conduct investigations of or to make arrests for offenses enumerated in this chapter, and any attorney authorized by law to prosecute or participate in the prosecution of such offenses;

**(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;

**(9)** “Judge of competent jurisdiction” means--

(a) a judge of a United States district court or a United States court of appeals; and

(b) a judge of any court of general criminal jurisdiction of a State who is authorized by a statute of that State to enter orders authorizing interceptions of wire, oral, or electronic communications;

**(10)** “communication common carrier” has the meaning given that term in section 3 of the Communications Act of 1934;

**(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;

**(12)** “electronic communication” means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include--

(A) any wire or oral communication;

(B) any communication made through a tone-only paging device;

(C) any communication from a tracking device (as defined in section 3117 of this title); or

(D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds;

**(13)** “user” means any person or entity who--

(A) uses an electronic communication service; and

(B) is duly authorized by the provider of such service to engage in such use;

**(14)** “electronic communications system” means any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications;

**(15)** “electronic communication service” means any service which provides to users thereof the ability to send or receive wire or electronic communications;

**(16)** “readily accessible to the general public” means, with respect to a radio communication, that such communication is not--

(A) scrambled or encrypted;

(B) transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of such communication;

(C) carried on a subcarrier or other signal subsidiary to a radio transmission;

(D) transmitted over a communication system provided by a common carrier, unless the communication is a tone only paging system communication; or

(E) transmitted on frequencies allocated under part 25, subpart D, E, or F of part 74, or part 94 of the Rules of the Federal Communications Commission, unless, in the case of a communication transmitted on a frequency allocated under part 74 that is not exclusively allocated to broadcast auxiliary services, the communication is a two-way voice communication by radio;

**(17)** “electronic storage” means--

(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and

(B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication;

**(18)** “aural transfer” means a transfer containing the human voice at any point between and including the point of origin and the point of reception;

**(19)** “foreign intelligence information”, for purposes of section 2517 (6) of this title, means--

(A) information, whether or not concerning a United States person, that relates to the ability of the United States to protect against--

(i) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(ii) sabotage or international terrorism by a foreign power or an agent of a foreign power; or

(iii) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

(B) information, whether or not concerning a United States person, with respect to a foreign power or foreign territory that relates to--

(i) the national defense or the security of the United States; or

(ii) the conduct of the foreign affairs of the United States;

**(20)** “protected computer” has the meaning set forth in section 1030; and

**(21)** “computer trespasser”--

(A) means a person who accesses a protected computer without authorization and thus has no reasonable expectation of privacy in any communication transmitted to, through, or from the protected computer; and

(B) does not include a person known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator of the protected computer for access to all or part of the protected computer.

**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) intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when--

(i) such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or

(ii) such device transmits communications by radio, or interferes with the transmission of such communication; or

(iii) such person knows, or has reason to know, that such device or any component thereof has been sent through the mail or transported in interstate or foreign commerce; or

(iv) such use or endeavor to use (A) takes place on the premises of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or (B) obtains or is for the purpose of obtaining information relating to the operations of any business or other

commercial establishment the operations of which affect interstate or foreign commerce; or

(v) such person acts in the District of Columbia, the Commonwealth of Puerto Rico, or any territory or possession of the United States;

(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) (i) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, intercepted by means authorized by sections 2511(2)(a)(ii), 2511(2)(b)-(c), 2511(2)(e), 2516, and 2518 of this chapter, (ii) knowing or having reason to know that the information was obtained through the interception of such a communication in connection with a criminal investigation, (iii) having obtained or received the information in connection with a criminal investigation, and (iv) with intent to improperly obstruct, impede, or interfere with a duly authorized criminal investigation, 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) a court order directing such assistance signed by the authorizing judge, or

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

(b) It shall not be unlawful under this chapter for an officer, employee, or agent of the Federal Communications Commission, in the normal course of his employment and in discharge of the monitoring responsibilities exercised by the Commission in the enforcement of chapter 5 of title 47 of the United States Code, to intercept a wire or electronic communication, or oral communication transmitted by radio, or to disclose or use the information thereby obtained.

(c) It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire, oral, or electronic communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception.

(d) It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.

(e) Notwithstanding any other provision of this title or section 705 or 706 of the Communications Act of 1934, it shall not be unlawful for an officer, employee, or agent of the United States in the normal course of his official duty to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, as authorized by that Act.

(f) Nothing contained in this chapter or chapter 121 or 206 of this title, or section 705 of the Communications Act of 1934, shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communications, or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing a means other than electronic surveillance as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, and procedures in this chapter or chapter 121 and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance, as defined in section 101 of such Act, and the interception of domestic wire, oral, and electronic communications may be conducted.

(g) It shall not be unlawful under this chapter or chapter 121 of this title for any person--

(i) to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public;

(ii) to intercept any radio communication which is transmitted--

(I) by any station for the use of the general public, or that relates to ships, aircraft, vehicles, or persons in distress;

(II) by any governmental, law enforcement, civil defense, private land mobile, or public safety communications system, including police and fire, readily accessible to the general public;

(III) by a station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio services; or

(IV) by any marine or aeronautical communications system;

(iii) to engage in any conduct which--

(I) is prohibited by section 633 of the Communications Act of 1934; or

(II) is excepted from the application of section 705(a) of the Communications Act of 1934 by section 705(b) of that Act;

(iv) to intercept any wire or electronic communication the transmission of which is causing harmful interference to any lawfully operating station or consumer electronic equipment, to the extent necessary to identify the source of such interference; or

(v) for other users of the same frequency to intercept any radio communication made through a system that utilizes frequencies monitored by individuals engaged in the provision or the use of such system, if such communication is not scrambled or encrypted.

(h) It shall not be unlawful under this chapter--

(i) to use a pen register or a trap and trace device (as those terms are defined for the purposes of chapter 206 (relating to pen registers and trap and trace devices) of this title); or

(ii) for a provider of electronic communication service to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire or electronic communication, or a user of that service, from fraudulent, unlawful or abusive use of such service.

(i) It shall not be unlawful under this chapter for a person acting under color of law to intercept the wire or electronic communications of a computer trespasser transmitted to, through, or from the protected computer, if--

(I) the owner or operator of the protected computer authorizes the interception of the computer trespasser's communications on the protected computer;

(II) the person acting under color of law is lawfully engaged in an investigation;

(III) the person acting under color of law has reasonable grounds to believe that the contents of the computer trespasser's communications will be relevant to the investigation; and

(IV) such interception does not acquire communications other than those transmitted to or from the computer trespasser.

**(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.

(b) A person or entity providing electronic communication service to the public may divulge the contents of any such communication--

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

(ii) with the lawful consent of the originator or any addressee or intended recipient of such communication;

(iii) to a person employed or authorized, or whose facilities are used, to forward such communication to its destination; or

(iv) which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency.

**(4)(a)** Except as provided in paragraph (b) of this subsection or in subsection (5), whoever violates subsection (1) of this section shall be fined under this title or imprisoned not more than five years, or both.

(b) Conduct otherwise an offense under this subsection that consists of or relates to the interception of a satellite transmission that is not encrypted or scrambled and that is transmitted--

(i) to a broadcasting station for purposes of retransmission to the general public; or

(ii) as an audio subcarrier intended for redistribution to facilities open to the public, but not including data transmissions or telephone calls, is not an offense under this subsection unless the conduct is for the purposes of direct or indirect commercial advantage or private financial gain.

[(c) Redesignated (b)]

**(5)(a)(i)** If the communication is--

(A) a private satellite video communication that is not scrambled or encrypted and the conduct in violation of this chapter is the private viewing of that communication and is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain; or

(B) a radio communication that is transmitted on frequencies allocated under subpart D of part 74 of the rules of the Federal Communications Commission that is not scrambled or encrypted and the conduct in violation of this chapter is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain, then the person who engages in such conduct shall be subject to suit by the Federal Government in a court of competent jurisdiction.

(ii) In an action under this subsection--

(A) if the violation of this chapter is a first offense for the person under paragraph (a) of subsection (4) and such person has not been found liable in a civil action under section 2520 of this title, the Federal Government shall be entitled to appropriate injunctive relief; and

(B) if the violation of this chapter is a second or subsequent offense under paragraph (a) of subsection (4) or such person has been found liable in any prior civil action under section 2520, the person shall be subject to a mandatory \$500 civil fine.

(b) The court may use any means within its authority to enforce an injunction issued under paragraph (ii)(A), and shall impose a civil fine of not less than \$500 for each violation of such an injunction.

## 18 U.S.C. 2520

### **§ 2520. Recovery of civil damages authorized**

**(a)** In general.--Except as provided in section 5211 (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) In an action under this section, if the conduct in violation of this chapter is the private viewing of a private satellite video communication that is not scrambled or encrypted or if the communication is a radio communication that is transmitted on frequencies allocated under subpart D of part 74 of the rules of the Federal Communications Commission that is not scrambled or encrypted and the conduct is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain, then the court shall assess damages as follows:

(A) If the person who engaged in that conduct has not previously been enjoined under section 2511(5) and has not been found liable in a prior civil action under this section, the court shall assess the greater of the sum of actual damages suffered by the plaintiff, or statutory damages of not less than \$50 and not more than \$500.

(B) If, on one prior occasion, the person who engaged in that conduct has been enjoined under section 2511(5) or has been found liable in a civil action under this section, the court shall assess the greater of the sum of actual damages suffered by the plaintiff, or statutory damages of not less than \$100 and not more than \$1000.

(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.

**(d) Defense.--**A good faith reliance on--

(1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization;

(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) or 2511(2)(i) of this title permitted the conduct complained of; is a complete defense against any civil or criminal action brought under this chapter or any other law.

**(e) Limitation.--**A civil action under this section may not be commenced later than two years after the date upon which the claimant first has a reasonable opportunity to discover the violation.

**(f) Administrative discipline.--**If a court or appropriate department or agency determines that the United States or any of its departments or agencies has violated any provision of this chapter, and the court or appropriate department or agency finds that the circumstances surrounding the violation raise serious questions about whether or not an officer or employee of the United States acted willfully or intentionally with respect to the violation, the department or agency shall, upon receipt of a true and correct copy of the decision and findings of the court or appropriate department or agency promptly initiate a proceeding to determine whether disciplinary action against the officer or employee is warranted. If the head of the department or agency involved determines that disciplinary action is not warranted, he or she shall notify the Inspector General with jurisdiction over the department or agency concerned and shall provide the Inspector General with the reasons for such determination.

**(g) Improper disclosure is violation.--**Any willful disclosure or use by an investigative or law enforcement officer or governmental entity of information

beyond the extent permitted by section 2517 is a violation of this chapter for purposes of section 2520(a).

**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--

(1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;

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

(3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;

(4) to a person employed or authorized or whose facilities are used to forward such communication to its destination;

(5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

(6) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 227 of the Victims of Child Abuse Act of 1990 (42 U.S.C. 13032);

(7) to a law enforcement agency--

(A) if the contents--

(i) were inadvertently obtained by the service provider; and

(ii) appear to pertain to the commission of a crime; or

[(B) Repealed. Pub.L. 108-21, Title V, § 508(b)(1)(A), Apr. 30, 2003, 117 Stat. 684]

[(C) Repealed. Pub.L. 107-296, Title II, § 225(d)(1)(C), Nov. 25, 2002, 116 Stat. 2157]

(8) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency.

**(c) Exceptions for disclosure of customer records.--**A provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a)(1) or (a)(2))--

(1) as otherwise authorized in section 2703;

(2) with the lawful consent of the customer or subscriber;

(3) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

(4) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency;

(5) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 227 of the Victims of Child Abuse Act of 1990 (42 U.S.C. 13032); or

(6) to any person other than a governmental entity.

**(d) Reporting of emergency disclosures.**--On an annual basis, the Attorney General shall submit to the Committee on the Judiciary of the House of Representatives and the Committee on the Judiciary of the Senate a report containing--

(1) the number of accounts from which the Department of Justice has received voluntary disclosures under subsection (b)(8); and

(2) a summary of the basis for disclosure in those instances where--

(A) voluntary disclosures under subsection (b)(8) were made to the Department of Justice; and

(B) the investigation pertaining to those disclosures was closed without the filing of criminal charges.

## **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.

**(d) Administrative discipline.**--If a court or appropriate department or agency determines that the United States or any of its departments or agencies has violated any provision of this chapter, and the court or appropriate department or agency finds that the circumstances surrounding the violation raise serious questions about whether or not an officer or employee of the United States acted willfully or intentionally with respect to the violation, the department or agency shall, upon receipt of a true and correct copy of the decision and findings of the court or appropriate department or agency promptly initiate a proceeding to determine whether disciplinary action against the officer or employee is warranted. If the head of the department or agency involved determines that disciplinary action is not warranted, he or she shall notify the Inspector General with jurisdiction over the department or agency concerned and shall provide the Inspector General with the reasons for such determination.

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

- (1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization (including a request of a governmental entity under section 2703(f) of this title);
- (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.

**(f) Limitation.**--A civil action under this section may not be commenced later than two years after the date upon which the claimant first discovered or had a reasonable opportunity to discover the violation.

**(g) Improper disclosure.**--Any willful disclosure of a 'record', as that term is defined in section 552a(a) of title 5, United States Code, obtained by an investigative or law enforcement officer, or a governmental entity, pursuant to section 2703 of this title, or from a device installed pursuant to section 3123 or 3125 of this title, that is not a disclosure made in the proper performance of the official functions of the officer or governmental entity making the disclosure, is a violation of this chapter. This provision shall not apply to information previously lawfully disclosed (prior to the commencement of any civil or administrative proceeding under this chapter) to the public by a Federal, State, or local governmental entity or by the plaintiff in a civil action under this chapter.

State of California )  
County of Los Angeles )  
)

Proof of Service by:  
US Postal Service  
✓ Federal Express

I, Stephen Moore, declare that I am not a party to the action, am over 18 years of age and my business address is: 354 South Spring St., Suite 610, Los Angeles, California 90013.

On 04/26/07 declarant served the within: Corrected Answering Brief of Plaintiffs-Appellees upon:

2 Copies ✓ FedEx USPS  
To each person listed on the next page.

Copies FedEx USPS

Copies FedEx USPS

Copies FedEx USPS

the address(es) designated by said attorney(s) for that purpose by depositing **the number of copies indicated above**, of same, enclosed in a postpaid properly addressed wrapper in a Post Office Mail Depository, under the exclusive custody and care of the United States Postal Service, within the State of California, or properly addressed wrapper in an Federal Express Official Depository, under the exclusive custody and care of Federal Express, within the State of California

I further declare that this same day the **original and** copies has/have been hand delivered for filing OR the **original and** 15 copies has/have been filed by ✓ third party commercial carrier for next business day delivery to:

Office of the Clerk  
United States Court of Appeals  
For the Ninth Circuit  
95 Seventh Street  
San Francisco, California 94103-1526

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

Signature: \_\_\_\_\_

## SERVICE LIST

<p>Peter D. Keisler Carl J. Nichols Anthony J. Coppolino Andrew H. Tannenbaum Joseph Hunt U.S. Department of Justice Civil Division, Federal Programs Branch 20 Massachusetts Avenue N.W. Room 6102 Washington, D.C. 20001 (202) 514-4782 (tel.) (202) 616-8470 (fax)</p>	<p>Douglas N. Letter Thomas M. Bondy Anthony A. Yang United States Department of Justice Civil Division, Appellate Statt 950 Pennsylvania Avenue N.W. Room 7513 Washington, D.C. 20530-0001 (202) 514-3602 (tel.) (202) 514-8151(fax)</p>
<p>Paul D. Clement Gregory G. Garre Daryl Joseffer Office of the Solicitor General 950 Pennsylvania Avenue NW Suite 5143 Washington, D.C. 20530-2201 (202) 514-2201 (tel.) (202) 514-3648 (fax)</p>	<p>Bruce A. Ericson Kevin M. Fong Marc H. Axelbaum Jacob R. Sorenson Pillsbury Winthrop Shaw Pittman LLP 50 Fremont Street San Francisco, CA 94105 (415) 983-1000 (tel.) (415) 983-1200 (fax)</p>
<p>Michael K. Kellogg Sean A. Lev Kellogg, Huber, Hansen, Todd, Evans &amp; Figel, P.L.L.C. 1615 M. Street, N.W., Suite 400 Washington, D.C. 20036 (202) 326-7900 (tel.) (202) 326-7999 (fax)</p>	<p>Bradford Berensen David Lawson Edward R. McNicholas Sidley Austin LLP 1501 K. Street, NW Washington D.C. 20005 (202) 736-8000 (tel.) (202) 736-8711 (fax)</p>