No. 06-17132

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

TASH HEPTING, *et al.*,

Plaintiffs-Appellees,

v.

AT&T CORP.,

Defendant-Appellant.

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

REPLY BRIEF OF APPELLANT AT&T CORP.

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

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

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

*Counsel of Record

May 24, 2007

Counsel for Defendant-Appellant AT&T Corp.

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES ii

INTRODUCTION 1

ARGUMENT 5

I. THE ISSUES REMAINING ON APPEAL HAVE BEEN NARROWED TO ALLEGATIONS CONCERNING A CONTENT "DRAGNET" 5

II. DISMISSAL AT THE THRESHOLD IS REQUIRED WHEN A CASE CANNOT BE FULLY AND FAIRLY LITIGATED WITHOUT STATE SECRETS 10

III. PLAINTIFFS' STANDING DEPENDS UPON PROOF OF A CONTENT "DRAGNET," WHICH CANNOT BE FULLY AND FAIRLY LITIGATED WITHOUT STATE SECRETS 18

A. The Validity of the Klein and Marcus Declarations Cannot Be Litigated 18

B. In Any Event, the Klein and Marcus Declarations Do Not Establish What Plaintiffs Claim 21

C. Plaintiffs Cannot Establish Their Standing by Claiming Mere "Risk" of Injury 26

IV. SECTION 1806(f) OF FISA DOES NOT APPLY HERE, AND IN ANY EVENT DOES NOT DISPLACE THE CONSTITUTIONALLY ROOTED STATE SECRETS PRIVILEGE 30

A. Section 1806(f) Does Not Apply to This Case 31

B. The State Secrets Privilege Is Not Displaced by FISA 36

CONCLUSION 39

CERTIFICATE OF COMPLIANCE

TABLE OF AUTHORITIES

Page

Cases

ACLU v. NSA, 438 F. Supp. 2d 754 (E.D. Mich. 2006) 6

ACLU Found. v. Barr, 952 F.2d 457 (D.C. Cir. 1991) 32, 34

Afshar v. Department of State, 702 F.2d 1125 (D.C. Cir. 1983) 7

Alfred A. Knopf, Inc. v. Colby, 509 F.2d 1362 (4th Cir. 1975) 7

American Library Ass'n v. FCC, 401 F.3d 489 (D.C. Cir. 2005) 28

Babbitt v. United Farm Workers Nat'l Union, 442 U.S. 289 (1979) 28

Baker & Hostetler LLP v. United States Dep't of Commerce, 473 F.3d 312 (D.C. Cir. 2006) 39

Baur v. Veneman, 352 F.3d 625 (2d Cir. 2003) 28

Bryant v. Yellen, 447 U.S. 352 (1980) 28

Central Delta Water Agency v. United States, 306 F.3d 938 (9th Cir. 2002) 28, 29

Churchill County v. Babbitt, 150 F.3d 1072, *amended on denial of reh'g*, 158 F.3d 491 (9th Cir. 1998) 28

City of Los Angeles v. Lyons, 461 U.S. 95 (1983) 26, 27, 29, 30

Clinton v. City of New York, 524 U.S. 417 (1998) 28

Covington v. Jefferson County, 358 F.3d 626 (9th Cir. 2004) 27, 28

Department of the Navy v. Egan, 484 U.S. 518 (1988) 37

Dimarzo v. Cahill, 575 F.2d 15 (1st Cir. 1978) 28

Edmonds v. United States Dep't of Justice, 323 F. Supp. 2d 65 (D.D.C. 2004), *aff'd mem.*, 161 F. App'x 6 (D.C. Cir.), *cert. denied*, 126 S. Ct. 734 (2005) 12

El-Masri v. United States, 479 F.3d 296 (4th Cir. 2007) 9, 10, 15, 17, 21, 25, 30, 36

Ellsberg v. Mitchell, 709 F.2d 51 (D.C. Cir. 1983) 11, 13

EPA v. Mink, 410 U.S. 73 (1973) 39

Farnsworth Cannon, Inc. v. Grimes, 635 F.2d 268 (4th Cir. 1980) 7, 11, 14

Fitzgerald v. Penthouse Int'l, Ltd., 776 F.2d 1236 (4th Cir. 1985) 11, 14

Fitzgibbon v. CIA, 911 F.2d 755 (D.C. Cir. 1990) 7, 10

Friends of the Earth, Inc. v. Gaston Copper Recycling Corp., 204 F.3d 149 (4th Cir. 2000) 28

Guong v. United States, 860 F.2d 1063 (Fed. Cir. 1988) 12

Halkin v. Helms:

598 F.2d 1 (D.C. Cir. 1978) ("*Halkin I*") 7, 8, 10, 11, 12, 13

690 F.2d 977 (D.C. Cir. 1982) ("*Halkin II*") 9, 11, 13, 17, 19, 29

Hall v. Norton, 266 F.3d 969 (9th Cir. 2001) 28

Helling v. McKinney, 509 U.S. 25 (1993) 27, 28

INS v. St. Cyr, 533 U.S. 289 (2001) 37

International Bhd. of Teamsters v. Transportation Sec. Admin., 429 F.3d 1130 (D.C. Cir. 2005) 28

Kasza v. Browner, 133 F.3d 1159 (9th Cir. 1998) 1, 14, 15, 16, 17, 19, 36, 39

LaDuke v. Nelson, 762 F.2d 1318 (1985), *amended*, 796 F.2d 309 (9th Cir. 1986) 29, 30

Maine People's Alliance v. Mallinckrodt, Inc., 471 F.3d 277 (1st Cir. 2006), *petition for cert. pending*, No. 06-1540 (U.S. filed May 16, 2007) 28

Military Audit Project v. Casey, 656 F.2d 724 (D.C. Cir. 1981) 8

Mountain States Legal Found. v. Glickman, 92 F.3d 1228 (D.C.Cir. 1996) 28

National Lawyers Guild v. Attorney General, 96 F.R.D. 390 (S.D.N.Y. 1982) 10

Nejad v. United States, 724 F. Supp. 753 (C.D. Cal. 1989) 12

O'Melveny & Myers v. FDIC, 512 U.S. 79 (1994) 34

Salisbury v. United States, 690 F.2d 966 (D.C. Cir. 1982) 9

Simon v. Eastern Ky. Welfare Rights Org., 426 U.S. 26 (1976) 28

Skillsky v. Lucky Stores, Inc., 893 F.2d 1088 (9th Cir. 1990) 22

Steel Co. v. Citizens for a Better Env't, 523 U.S. 83 (1998) 19

Sterling v. Tenet, 416 F.3d 338 (4th Cir. 2005), *cert. denied*, 126 S. Ct. 1052 (2006) 10, 11, 12, 17, 25, 30

Sutton v. St. Jude Med. S.C., Inc., 419 F.3d 568 (6th Cir. 2005) 28

Tenet v. Doe, 544 U.S. 1 (2005) 7, 15

Terkel v. AT&T Corp., 441 F. Supp. 2d 899 (N.D. Ill. 2006) 6, 7, 9

Totten v. United States, 92 U.S. 105 (1876) 7, 15, 30

United States, In re, 872 F.2d 472 (D.C. Cir. 1989) 13, 16, 17

United States v. Cavanagh, 807 F.2d 787 (9th Cir. 1987) 32-33

United States v. Damrah, 412 F.3d 618 (6th Cir. 2005) 33

United States v. Isa, 923 F.2d 1300 (8th Cir. 1991) 33

United States v. Johnson, 952 F.2d 565 (1st Cir. 1991) 33

United States v. Karo, 468 U.S. 705 (1984) 23

United States v. Nixon, 418 U.S. 683 (1974) 37

United States v. Ott, 827 F.2d 473 (9th Cir. 1987) 32

United States v. Pawlinski, 374 F.3d 536 (7th Cir. 2004) 28

United States v. Pelton, 696 F. Supp. 156 (D. Md. 1986) 6-7

United States v. Reynolds, 345 U.S. 1 (1953) 7, 8, 16, 17, 37, 38, 39

United States v. Texas, 507 U.S. 529 (1993) 36

United States ex rel. Ross v. LaVallee, 341 F.2d 823 (2d Cir. 1965) 27

Village of Elk Grove Village v. Evans, 997 F.2d 328 (7th Cir. 1993) 28

Webster v. Doe, 486 U.S. 592 (1988) 17

Weston v. Lockheed Missiles & Space Co., 881 F.2d 814
(9th Cir. 1989) 14

Zuckerbraun v. General Dynamics Corp.:

755 F. Supp. 1134 (D. Conn. 1990), *aff'd*, 935 F.2d 544
(2d Cir. 1991) 12

935 F.2d 544 (2d Cir. 1991) 11, 12, 26, 30

Zweibon v. Mitchell, 516 F.2d 594 (D.C. Cir. 1975) 39

Constitution, Statutes, and Rules

U.S. Const.:

Art. III 14, 25, 27

Amend. IV 29

Amend. VIII 27

Communications Assistance for Law Enforcement Act,
47 U.S.C. §§ 1001 *et seq.* 25

47 U.S.C. § 1002(a) 25

Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508,
100 Stat. 1848:

18 U.S.C. § 2510(11) 27

18 U.S.C. § 2511(3)(a) 22

18 U.S.C. § 2519 9

18 U.S.C. § 2520(a) 27

18 U.S.C. § 2520(d) 22

18 U.S.C. § 2702(a)(1) 22

18 U.S.C. § 2707(a) 27

18 U.S.C. § 2707(e) 22

18 U.S.C. § 2711(1) 27

Federal Tort Claims Act, 28 U.S.C. §§ 2671 *et seq.* 39

Foreign Intelligence Surveillance Act of 1978,
50 U.S.C. §§ 1801 *et seq.*:

50 U.S.C. § 1801(f) 10, 22

50 U.S.C. § 1801(g) 35

50 U.S.C. § 1801(k) 27, 31

50 U.S.C. § 1805(i) 22

50 U.S.C. § 1806 .... 33, 34

50 U.S.C. § 1806(c) 33

50 U.S.C. § 1806(d) 33

50 U.S.C. § 1806(e) 33

50 U.S.C. § 1806(f) .... *passim*

50 U.S.C. § 1806(g) 33

50 U.S.C. § 1806(j) 33, 34

50 U.S.C. § 1807 9

50 U.S.C. § 1808 9

50 U.S.C. § 1826 9

50 U.S.C. § 1846 9

50 U.S.C. § 1862 9

Freedom of Information Act, 5 U.S.C. § 552 .... 7, 13, 39

Resource Conservation and Recovery Act of 1976,
42 U.S.C. §§ 6901 *et seq.* 39

47 U.S.C. § 605(a) 22, 27

47 U.S.C. § 605(e)(3)(A) 27

Fed. R. Civ. P.:

Rule 56(e) 22

Rule 56(f) 16

Legislative Materials

H.R. Rep. No. 95-1283, pt. 1 (1978) 10

S. Rep. No. 95-604, pt. 1 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3904 .... 34, 38

S. Rep. No. 95-701 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3973 .... 10, 38

Other Authorities

Brief of Plaintiffs-Appellants, *Kasza v. Browner*, 1996 WL 33418896 (9th Cir. Docket Nos. 96-15535 & 96-15537) 19

Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531 (2005) 23

Richard A. Posner, *Not a Suicide Pact: The Constitution in a Time of National Emergency* (2006) 23

INTRODUCTION

It is undisputed that, in order to establish standing, Plaintiffs must show both that AT&T participated in an illegal program of electronic surveillance and that, as a result, Plaintiffs' communications were disclosed to the government. There is also no dispute that, in a sworn statement filed in this case, the Director of National Intelligence has identified both those issues as being covered by the state secrets privilege. Under this Court's precedents, the Court must give "utmost deference" to that solemn determination by the nation's highest intelligence officer. *Kasza v. Browner*, 133 F.3d 1159, 1166 (9th Cir. 1998).

Instead of applying that binding standard and dismissing the case because the state secrets doctrine prevents litigation of the facts essential to proving Plaintiffs' standing, the district court relied on a chain of speculation and inference to surmise that AT&T participated in NSA surveillance activities and that those alleged activities were so broad that they must necessarily have encompassed Plaintiffs. Plaintiffs cannot and do not defend the district court's analysis. Moreover, they concede that they are not challenging the targeted Terrorist Surveillance Program ("TSP"), and they make no serious effort to defend their call records claims. The focus of Plaintiffs' submission is now entirely on their allegations of an indiscriminate content surveillance "dragnet." Their arguments as to why such claims can proceed depend on a novel conceptual framework that is

not reflected in the district court's ruling – and that contains three fundamental fallacies.

The first fallacy is Plaintiffs' procedural framework for evaluating when cases implicating state secrets must be dismissed. In Plaintiffs' view, a court must advance such cases as far as possible, even when it is clear at the outset that the state secrets assertion will prevent the claims from being proven or the defendant from responding to the allegations – and notwithstanding the danger to national security that courts recognize must be the foremost concern in such cases. This argument is both unprecedented and misguided. It is established law, in this and every other circuit to consider the question, that the national security implications of state secrets cases demand a cautious approach. A state secrets case must be dismissed *as soon as* it becomes clear that the removal of state secrets from the case will prevent litigation of the claims or defenses. Any other rule threatens national security, is wasteful of party and judicial resources, and is unfair to defendants that have to fight with their hands tied behind their backs.

That rule requires dismissal in this case *now* because the parties in this case simply cannot litigate whether Plaintiffs' communications were swept up in a clandestine NSA content dragnet using AT&T's facilities. Indeed, to the extent that Plaintiffs' assertion (at 1) that their claims regarding "the most extensive surveillance dragnet in American history" are "unrebutted" is true, that is only

because, once the government asserted the state secrets privilege, AT&T was deprived of the ability to defend itself against Plaintiffs' allegations. Plaintiffs' statement thus demonstrates why this case should be dismissed, and dismissed now.

Plaintiffs' second fallacy is their supposition (at 68) that the Klein and Marcus declarations must be taken as gospel truth and "prove[] . . . to a near certainty" "that AT&T has diverted their personal communications and records to the NSA." These declarations may not be true; they may not be accurate; or they may present only an incomplete or distorted version of the truth. Klein was a line technician who never held a security clearance, never had access to the "secret room" he purports to describe, and never possessed any state secrets. (That, not abandonment of the privilege, is of course why the government did not assert the state secrets privilege over the declarations.) But the accuracy and evidentiary value of the declarations cannot be litigated, because the United States' state secrets assertion prevents AT&T from saying anything in response. Moreover, even on their own terms, these declarations, which are shot through with inadmissible hearsay, do not establish that the NSA captured all of the Internet traffic on AT&T's backbone or examined any particular communications, including Plaintiffs'. It is simply preposterous to suggest that Klein's guesses based on leaky air conditioners, and Marcus's musings about Klein's guesses, have

"proved . . . to a near certainty" that "the Government intercepted communications . . . of millions and millions of Americans[] without suspicion." Hepting Br. 55, 68.

Finally, Plaintiffs seek a panacea for all the flaws in their position by arguing that § 1806(f) of FISA *sub silentio* displaced the constitutionally rooted state secrets privilege in all litigation concerning foreign intelligence surveillance. But, far from being "expressly anticipated" by Congress, as Plaintiffs assert (at 32), this argument finds *no* hint of support in FISA's text or its legislative history – neither of which in any way even suggests that Congress intended to displace the state secrets doctrine. Nor has this subsection of FISA *ever*, in its almost 30 years of existence, been so applied or interpreted by any court. Beyond that, the argument ignores the fact that § 1806(f) serves a very different function than the state secrets doctrine. Section 1806(f), unlike the state secrets privilege, does not require a court to consider national security interests; on the contrary, Congress contemplated that the Executive ordinarily would retain authority to weigh those interests itself.

In any event, it is unnecessary for this Court to address this argument, because § 1806(f) does not apply here. First, Plaintiffs cannot show that they are "aggrieved persons," as § 1806(f) on its face requires. Second, and independently, § 1806(f) applies *only* when the Attorney General invokes it, which has not

occurred here. Plaintiffs ignore these requirements and attempt to transform § 1806(f) from a shield the government can use to protect information regarding acknowledged surveillance from public disclosure, into a sword in the hands of those who seek to confirm suspicions that they may have been surveilled. No court has *ever* interpreted § 1806(f) in this fashion.

ARGUMENT

I. THE ISSUES REMAINING ON APPEAL HAVE BEEN NARROWED TO ALLEGATIONS CONCERNING A CONTENT "DRAGNET"

Plaintiffs' brief has substantially narrowed the issues in this case. The litigation below and other related lawsuits put at issue three categories of alleged surveillance: (1) the TSP; (2) an alleged broader program of untargeted "dragnet" content surveillance; and (3) an alleged call records program. AT&T Br. 7-12.

Plaintiffs have now affirmatively abandoned the TSP. They concede (at 82) that that "conduct . . . is not at issue in this case" and repeatedly emphasize (*e.g.*, at 1) that they are challenging a much broader alleged "dragnet" program, *not* a targeted program of surveilling international communications where there is a reasonable basis to conclude that one party is assisting al Qaeda. Thus, their case now stands bereft of the only post-9/11 NSA surveillance program whose existence the United States has ever acknowledged.

Plaintiffs also make no meaningful effort to defend their allegations of a call records program. They do not dispute that the state secrets privilege was validly

invoked as to these allegations or that the declarations submitted by the Director of National Intelligence and the Director of the NSA cover every aspect of the alleged call records program – including its existence, whether AT&T participated, whether Plaintiffs were targets of any such program, and all operational details. Plaintiffs likewise do not defend the district court's decision to retain jurisdiction over the call records claims notwithstanding its conclusion that these claims cannot proceed. *See* AT&T Br. 56-59. Instead, in two scant pages of their 90-page submission, Plaintiffs claim that the call records program is not a secret because, they say, its "facts [are] splayed across the front pages of newspapers." Hepting Br. 43.

Reliance on such hearsay media reports, which may or may not be accurate, has been rejected by every court to consider the matter, including the court below. Such reports do not constitute official acknowledgement of even the mere existence of a call records program, much less do they establish the kind of operational details that would be necessary to litigate this case.[1] Because "there is a difference between speculation and confirmation," such reports cannot vitiate the state secrets privilege. *United States v. Pelton*, 696 F. Supp. 156, 158 (D. Md.

---

[1] *See Terkel v. AT&T Corp.*, 441 F. Supp. 2d 899, 908-20 (N.D. Ill. 2006); *Hepting v. AT&T Corp.*, 439 F. Supp. 2d 974, 997 (N.D. Cal. 2006) (ER 328); *ACLU v. NSA*, 438 F. Supp. 2d 754, 765 (E.D. Mich. 2006).

1986); *accord Alfred A. Knopf, Inc. v. Colby*, 509 F.2d 1362, 1370 (4th Cir. 1975); *Terkel*, 441 F. Supp. 2d at 914. Thus, under the national security exception to the Freedom of Information Act ("FOIA") – which is persuasive in this context[2] – documents are protected from release unless there is "an *official* and *documented* disclosure." *Fitzgibbon v. CIA*, 911 F.2d 755, 765 (D.C. Cir. 1990) (emphases added); *see Afshar v. Department of State*, 702 F.2d 1125, 1130-31, 1133-34 (D.C. Cir. 1983). This conclusion follows *a fortiori* from the Supreme Court's refusal to find the state secrets privilege waived even in cases in which plaintiffs have asserted *first-hand knowledge* of state secrets through personal participation in intelligence activities. *See Tenet v. Doe*, 544 U.S. 1, 6 (2005); *United States v. Reynolds*, 345 U.S. 1, 7-8 (1953); *Totten v. United States*, 92 U.S. 105 (1876); *accord Farnsworth Cannon, Inc. v. Grimes*, 635 F.2d 268, 281 (4th Cir. 1980) (en banc) (per curiam). Any contrary rule would allow the protections that exist for classified intelligence activities to be voided by unauthoritative, hearsay statements.

Nor is the result any different because Plaintiffs now cite (at 11-12) statements attributed to members of Congress. Many of these statements were not before the district court. *E.g.*, SER 818-45. Some do not even relate to the alleged

---

[2] *See Halkin v. Helms*, 598 F.2d 1, 9 (D.C. Cir. 1978) ("*Halkin I*"); *Terkel*, 441 F. Supp. at 914 n.9.

call records program. *E.g.*, SER 745-46, 832. In any event, none of these statements to reporters involves confirmation by an official of the Executive Branch, which would necessarily operate the alleged program, much less by "the head of the department which has control over the matter." *Reynolds*, 345 U.S. at 8; *cf. Military Audit Project v. Casey*, 656 F.2d 724, 744-45 (D.C. Cir. 1981) (unofficial disclosures do not undermine state secrets).

Hearsay statements by individual legislators who, by definition, do not actually run intelligence programs are neither authoritative nor reliable. These statements may well be inaccurate in whole or in part, and, in any event, they provide no basis to override the judgment of the Director of National Intelligence that the matters at issue here involve state secrets. Indeed, disclosures of national security information by Congress in an *official* forum and with far greater thoroughness than what is reported here have been held insufficient to remove state secrets protection. *See Halkin I*, 598 F.2d at 10 (rejecting the argument that, because "congressional committees investigating intelligence matters had revealed so much information," the state secrets privilege was inapplicable). Any other rule would create perverse incentives for congressional leaks of national security information by dissenting legislators, and concomitant disincentives for briefings of Congress by the Executive that form the principal means by which oversight of and democratic accountability for secret intelligence programs are typically

ensured. *See, e.g.*, *Terkel*, 441 F. Supp. 2d at 914; *see also* 18 U.S.C. § 2519; 50 U.S.C. §§ 1807, 1808, 1826, 1846, 1862 (requiring reports to Congress and the Administrative Office of the United States Courts).

The normal rule applies with particular force here because the remarks attributed to individual legislators do not purport to reveal any operational details of the alleged program. Indeed, many of the quotes are pulled out of context from larger quotes in which members of Congress specifically refused to provide details or even affirmatively denied the type of data-mining alleged by Plaintiffs. *E.g.*, SER 720, 824. Such limited disclosure cannot establish Plaintiffs' standing, because it cannot waive privilege over the specific facts relevant to determining whether the alleged program harmed any concrete interest of Plaintiffs. *See El-Masri v. United States*, 479 F.3d 296, 308-09, 311 (4th Cir. 2007); *Terkel*, 441 F. Supp. 2d at 915-17, 919-20; *see also Halkin v. Helms*, 690 F.2d 977, 994 (D.C. Cir. 1982) ("*Halkin II*") (rejecting "the theory that 'because *some* information about the project ostensibly is now in the public domain, *nothing* about the project . . . can properly remain classified' or otherwise privileged from disclosure") (citation omitted); *Salisbury v. United States*, 690 F.2d 966, 971 (D.C. Cir. 1982) ("[B]are discussions by . . . the Congress of NSA's methods generally cannot be equated with disclosure by the agency itself of its methods of

information gathering."); *Fitzgibbon*, 911 F.2d at 765; *Halkin I*, 598 F.2d at 10; *National Lawyers Guild v. Attorney General*, 96 F.R.D. 390, 402 (S.D.N.Y. 1982).

Plaintiffs also assert, in one sentence (at 35), that their call records claims can proceed under § 1806(f). Even leaving aside the other fundamental problems with their § 1806(f) argument, *see infra* Part IV, § 1806(f) covers only "electronic surveillance," the statutory definition of which includes only content intercepted while in transmission through wire, radio, or bugging devices. *See* 50 U.S.C. § 1801(f); *see also* H.R. Rep. No. 95-1283, pt. 1, at 51 (1978) ("[e]xamination of telephone billing records in documentary form is not covered" under FISA's definition of "electronic surveillance"); S. Rep. No. 95-701, at 35-36 (1978) (same), *reprinted in* 1978 U.S.C.C.A.N. 3973, 4004-05.

II. DISMISSAL AT THE THRESHOLD IS REQUIRED WHEN A CASE CANNOT BE FULLY AND FAIRLY LITIGATED WITHOUT STATE SECRETS

Plaintiffs argue that it is premature to dismiss their challenge to the one alleged program still at issue – the supposed content "dragnet" – because this case is only at the "pleading stage." Plaintiffs are wrong on the law.

The dispositive principle here is a simple one: in a case involving state secrets, the court must dismiss as soon as it becomes apparent that the case will not be able to be fully and fairly litigated. *See El-Masri*, 479 F.3d at 306; *Sterling v. Tenet*, 416 F.3d 338, 346-47 (4th Cir. 2005), *cert. denied*, 126 S. Ct. 1052 (2006);

Zuckerbraun v. General Dynamics Corp., 935 F.2d 544, 547-48 (2d Cir. 1991); *Fitzgerald v. Penthouse Int'l, Ltd.*, 776 F.2d 1236, 1243 (4th Cir. 1985); *Halkin II*, 690 F.2d at 999; *Farnsworth Cannon*, 635 F.2d at 281; AT&T Br. 26-31 & n.12. This is not an argument, contrary to the strawman Plaintiffs repeatedly assault, that "Plaintiffs must *prove* their standing at this early stage of the litigation," Hepting Br. 69, 73-74, but rather a simple consequence of the "evidentiary" nature of the privilege: when the effect of the state secrets privilege is to remove evidence from a case without which full and fair litigation of the claims *or* defenses becomes impossible, dismissal is required. Plaintiffs here would have to prove their standing in due course – and AT&T would have to be afforded an opportunity to contest any such showing – but we know *now* that litigation over standing will be impossible without access to state secrets. Under such circumstances, dismissal is required. *See Sterling*, 416 F.3d at 344 ("Once the judge is satisfied that there is a 'reasonable danger' of state secrets being exposed," the court is "not required to play with fire and chance further disclosure – inadvertent, mistaken, or even intentional – that would defeat the very purpose for which the privilege exists.").

Plaintiffs note (at 53-54, 82-86) that some of the state secrets cases discussed in our opening brief – *Halkin I*, *Halkin II*, and *Ellsberg v. Mitchell*, 709 F.2d 51 (D.C. Cir. 1983) – proceeded beyond the pleading stage. In fact, courts have dismissed numerous state secrets cases at the outset, including relevant claims in

Halkin I (598 F.2d at 10).[3] Plaintiffs' contrary claim (at 2) that dismissal at the outset "is almost never granted" is undermined by their own *amici*, which identify ***19*** state secrets cases that were dismissed prior to *any* discovery. *See* Weaver Br. Add. (col. 2). These cases all support and demonstrate the rule set forth above – that, whatever the procedural posture, a case implicating state secrets must be dismissed as soon as it becomes clear that it cannot be litigated to conclusion.[4]

No case supports the proposition that a case should proceed through discovery once it is evident that it will be impossible to litigate central (indeed, in this case, jurisdictional) issues without disclosing state secrets. Certainly the cases on which Plaintiffs rely do not fall into this category. In *Halkin I*, the plaintiffs obtained "a limited amount of discovery" in the form of interrogatories concerning only the government's state secrets assertion itself. 598 F.2d at 5. Directly relevant here, however, that court denied discovery on the "vital" fact of whether the plaintiffs' communications had been acquired, because that fact was a state

---

[3] *E.g.*, *Sterling*, 416 F.3d at 348; *Zuckerbraun*, 935 F.2d at 548, *aff'g* 755 F. Supp. 1134, 1140 (D. Conn. 1990); *Guong v. United States*, 860 F.2d 1063, 1064, 1065-66 (Fed. Cir. 1988); *Edmonds v. United States Dep't of Justice*, 323 F. Supp. 2d 65, 68, 81-82 (D.D.C. 2004), *aff'd mem.*, 161 F. App'x 6 (D.C. Cir.), *cert. denied*, 126 S. Ct. 734 (2005); *Nejad v. United States*, 724 F. Supp. 753, 757 (C.D. Cal. 1989).

[4] The cases cited by Plaintiffs (at 23 n.4) follow this rule. They are further examples of the uncontroversial proposition that the state secrets privilege may require dismissal at different stages of the litigation in different cases – just like the cases we cited (at 26-27 n.12) for the same proposition.

secret, and it dismissed on the pleadings. *Id.* at 6, 7; *see also Halkin II*, 690 F.2d at 984 (discussing *Halkin I*). In *Halkin II*, discovery was permitted only as to matters the government deemed non-secret. 690 F.2d at 984-87 & n.28; *id.* at 1005 (noting "*documented* instances of . . . surveillance") (emphasis added). Once the state secrets privilege was invoked against discovery of additional information, the court dismissed because the plaintiffs were "incapable of making the showing necessary to establish their standing." *Id.* at 998; *see id.* at 999 ("[a]ppellants have alleged, but *ultimately cannot show*, a concrete injury").[5]

Once the government asserts the privilege, dismissal is appropriate *at that time* if the plaintiff's case cannot be litigated or the defendant cannot defend itself. That is precisely the situation here. Just as in the *Halkin* decisions, the United States has invoked the state secrets privilege over basic aspects of the litigation, and any meaningful discovery Plaintiffs might take would necessarily implicate those state secrets. AT&T can neither respond to discovery requests nor defend itself against any allegations about whether or not it cooperated in a classified program without revealing what the government's chief intelligence official has

[5] *See also Ellsberg*, 709 F.2d at 53-54, 55 & n.13, 65 (case dismissed where question of which plaintiffs were surveilled was state secret). Plaintiffs rely heavily (at 21-23) on *In re United States*, 872 F.2d 472 (D.C. Cir. 1989), to advocate pushing ahead, but that case arose on mandamus and involved old allegations and stale evidence, most of which the plaintiff already possessed through FOIA. *Id.* at 478-79.

concluded are state secrets. Accordingly, it is clear that the threshold Article III requirement of standing cannot be litigated without revealing state secrets, and the case should be dismissed now.

Plaintiffs' misunderstanding of the procedural law relevant to state secrets results in several further errors. *First*, they assert (at 19-20) that dismissal on the pleadings is appropriate only when the "very subject matter" of a case is a state secret but not, by implication, in any other circumstance where full and fair litigation would be impossible without state secrets. This suggestion has no support. They rely exclusively (at 19) on a bare citation to *Kasza*, but *Kasza* announces no such limitation. Far from it: *Kasza* reaffirms *Weston v. Lockheed Missiles & Space Co.*, 881 F.2d 814, 816 (9th Cir. 1989), and *Weston* depends on *Fitzgerald*, which holds that a case must be dismissed when " 'the privilege so far obstructs normal proof in respect of the issues presented by the parties as to deprive the litigation process of its essential utility for fair resolution of those issues,' " 776 F.2d at 1241-42 (quoting *Farnsworth Cannon*, 635 F.2d at 280). Indeed, *Fitzgerald* makes clear that a "very subject matter" case is just one in which "there was simply no way [the] case could be tried without compromising sensitive military secrets." *Id.* at 1243. That is precisely the circumstance here, where a trial (or any other proceeding) as to whether AT&T assisted in this alleged "dragnet" program and whether Plaintiffs' communications were intercepted under

such a program would compromise what the Director of National Intelligence has identified in his sworn statement as state secrets. *See also El-Masri*, 479 F.3d at 310 (the "'very subject matter' of a civil proceeding, for purposes of our dismissal analysis, are those facts necessary to litigate it – not merely to discuss it in general terms").[6] Thus, far from supporting Plaintiffs, *Kasza* itself suggests a case should not go forward where, as here, "any further proceeding . . . would jeopardize national security" and "[n]o protective procedure can salvage" the litigation. 133 F.3d at 1170.

Second, even if dismissal were appropriate on the pleadings only in a "very subject matter" case, dismissal still would be required here, because, as Plaintiffs admit, the government's state secrets assertion encompasses the very subject matter of this case. Plaintiffs themselves aver that "the subject matter of this action is whether AT&T participated in an illegal program of electronic surveillance." Hepting Br. 24; *see also id.* at 17. But the United States has asserted the state secrets privilege over precisely these matters – *viz.*, "allegations concerning intelligence activities, sources, methods, relationships, or targets," including

[6] Plaintiffs suggest in passing (at 24 n.5) that *Tenet v. Doe* drastically narrowed the state secrets doctrine, so that dismissal on the pleadings "may only be available where the *Totten* jurisdictional bar applies." Even leaving aside that this case does involve *Totten*, *see* U.S. Br. 17-20, the argument is meritless. In *Tenet*, the Court held that *Totten* and state secrets are separate, coexisting doctrines. 544 U.S. at 9-10.

"allegations about NSA's purported involvement with AT&T." Negroponte Decl. ¶ 12 (ER 58); *accord* Alexander Decl. ¶ 8 (ER 64). Accordingly, even on Plaintiffs' view of the case, this Court could affirm *only* by rejecting the judgment of the Director of National Intelligence and the Director of the NSA that whether AT&T participated in an alleged content "dragnet" is a state secret. We are unaware of any case in which any court has so starkly overridden the "'utmost deference'" that must be afforded to the judgments of the nation's most senior intelligence officials regarding the national security implications of publicly disclosing information about alleged intelligence activities, *Kasza*, 133 F.3d at 1166 (quoting *In re United States*, 872 F.2d at 475, and citing *Reynolds*, 345 U.S. at 10), and Plaintiffs proffer none.

Finally, even if it were improper to dismiss this case on the pleadings (and it is not), that is irrelevant, because the United States also moved for summary judgment. SER 655. This point is not susceptible to dispute, and Plaintiffs do not dispute it. *See* Hepting Br. 15.[7]

In the end, it is clear that Plaintiffs' cramped view of the state secrets privilege derives from simple hostility to the privilege itself. Hepting Br. 55-58;

---

[7] Plaintiffs' Rule 56(f) declaration is a red herring. Hepting Br. 73. The fact that they requested materials protected by the government's state secrets assertion, *see* SER 589-91, cannot defeat the assertion of that very privilege.

accord NAACP Br. 11-12, 19-20. They suggest that this Court has a "responsibility" greater than applying the settled principles of this doctrine, Hepting Br. 55, and that applying those principles raises the specter of a right without a remedy, *id.* at 56-57 (citing *Webster v. Doe*, 486 U.S. 592 (1988)). Not so. When a constitutional privilege is validly invoked, judicial review is not precluded. *See El-Masri*, 479 F.3d at 312. Rather, the state secrets privilege is a substantive rule of law that operates to remove certain evidence from litigation. When the unavailable evidence is critical to full and fair litigation – including, as here, the ability of a defendant to respond to central allegations that Plaintiffs must establish for the court to have jurisdiction – the case must be dismissed. When litigation terminates under these circumstances, it is not because the Executive has improperly interfered with the judicial function; rather, it is because the Supreme Court, this Court, and every court to address the question has recognized that, where state secrets are at issue, national security concerns must be foremost, such that " 'even the most compelling necessity cannot overcome the claim of privilege.' " *Kasza*, 133 F.3d at 1166 (quoting *Reynolds*, 345 U.S. at 11); *accord Sterling*, 416 F.3d at 344-45; *In re United States*, 872 F.2d at 476; *Halkin II*, 690 F.2d at 990, 999 n.81 ("Just as standing cannot be denied because of the relatively modest quantum of the injury, it cannot be upheld merely on the basis of the importance of the injury alleged.") (citations omitted).

III. PLAINTIFFS' STANDING DEPENDS UPON PROOF OF A CONTENT "DRAGNET," WHICH CANNOT BE FULLY AND FAIRLY LITIGATED WITHOUT STATE SECRETS

The law requires dismissal here because the parties cannot litigate the necessary factual predicates to Plaintiffs' standing – namely, that the NSA conducted a content "dragnet," that AT&T participated in it, and that AT&T divulged to the NSA the named plaintiffs' communications. *See* AT&T Br. 31-33, 43-53. In arguing to the contrary, Plaintiffs make no effort to defend the chain of suppositions on which the district court relied. Instead, Plaintiffs now rely entirely on something the district court wisely rejected: Klein's declaration, and Marcus's gloss on it. *Compare Hepting*, 439 F. Supp. 2d at 990-91 (ER 322-23).

A. The Validity of the Klein and Marcus Declarations Cannot Be Litigated

First and foremost, Plaintiffs' reliance on Klein's and Marcus's declarations is legally insufficient because AT&T cannot defend itself by litigating the validity of their allegations. Invocation of the state secrets privilege does not mean that Plaintiffs' unprivileged evidence must be accepted as "unrebutted" and therefore true and accurate. Hepting Br. 1, 3, 62. AT&T cannot respond to allegations made by Klein and Marcus, because doing so would require confirming or denying the alleged program, AT&T's alleged participation in it, and its operational details –

all of which the United States has asserted are state secrets.[8] When the exclusion of evidence means that fundamental aspects of the case cannot be litigated – such as elements, defenses, or, as here, standing – then the case must be dismissed. *See Kasza*, 133 F.3d at 1166; *see also Halkin II*, 690 F.2d at 1000 ("With no hope of a complete record and adversarial development of the issue, we cannot authorize such inquiry."); AT&T Br. 51-52. In *Kasza* itself, the plaintiffs argued to this Court that their case should go forward despite the government's invocation of the state secrets privilege in part because of sworn "affidavits from workers" that created factual disputes regarding issues over which privilege had been claimed. Brief of Plaintiffs-Appellants at 22-24, *Kasza v. Browner*, 1996 WL 33418896, at *22-*24 (9th Cir. Docket Nos. 96-15535 & 96-15537). This Court nevertheless affirmed the dismissal on the basis of state secrets and disallowed further discovery or litigation without even mentioning this evidence.

Because Plaintiffs rely entirely on the Klein and Marcus declarations to claim they can establish standing without state secrets, they have no choice but to

---

[8] Contrary to Plaintiffs' assertion (at 64), this issue was both raised and considered below. The district court stated that AT&T's asserted inability to "raise a valid defense" did not preclude Plaintiffs from pursuing "at least some discovery," and noted the government's argument that state secrets "effectively deprives AT&T of information necessary to raise valid defenses." 439 F. Supp. 2d at 985, 994 (ER 317, 326). In any event, standing defects of this sort are jurisdictional and can be raised at any time. *See Steel Co. v. Citizens for a Better Env't*, 523 U.S. 83, 95 (1998).

seek to circumvent the fundamental principle that a case must be dismissed when a central aspect of it cannot be litigated fully and fairly. They do so by arguing (at 37-43, 65-66) that what (if anything) occurred in the AT&T facility described by Klein is not a state secret, and thus that AT&T can in fact respond. In particular, Plaintiffs contend (at 65-66) that, by not asserting state secrets over Klein's declaration, the United States engaged in a subject-matter waiver as to any and all details of the alleged "dragnet."

Plaintiffs do not cite a single state secrets case to support the proposition that failure to assert the privilege with respect to a particular piece of evidence proffered by a third party waives the privilege with respect to the entirety of the classified intelligence program the third party purports to describe. Indeed, directly contrary to Plaintiffs' theory, case law establishes that even disclosure by *official* sources of *some* information does not throw open the doors to litigation and attendant discovery of other undisclosed information on the same subject. *See supra* pp. 9-10.

Moreover, the government has explained that it did not assert the state secrets privilege over these declarations because Klein and Marcus "never had access to any of the relevant classified information here, and with all respect to them, through no fault or failure of their own, they don't know anything." ER 189. The fact that those two *claim* to know something neither means that they in fact do

nor, more importantly, that the truth or falsity of their allegations can be litigated without divulging state secrets. Put differently, that Klein's claims are not state secrets does not mean that *responding* to them would not require state secrets. Even if Klein were absolutely wrong about everything he believes he saw, explaining what *isn't* happening would require AT&T to explain what, if anything, *is* happening. Even if the answer were "nothing," that answer would be precluded by the state secrets assertion. *See El-Masri*, 479 F.3d at 309. The crucial point is that, because of the state secrets doctrine, AT&T is utterly unable to defend itself against the "dragnet" allegations that form the basis for Plaintiffs' claim of standing. Unless the government's state secrets invocation is overridden – which neither Plaintiffs nor the district court have even claimed can be done – then the case has a fatal defect that renders it non-justiciable.

B. In Any Event, the Klein and Marcus Declarations Do Not Establish What Plaintiffs Claim

In any event, even on their own terms, the Klein and Marcus declarations do not establish what Plaintiffs assert they do.

As a threshold matter, the declarations do not contain competent evidence, much less "eyewitness testimony." Hepting Br. 5. Most of the central assertions relating to the NSA in Klein's declaration are rank hearsay, repeating the statements of an unidentified co-worker. *E.g.*, Klein Decl. ¶¶ 10 ("FSS #1 told me"; "FSS #1 later confirmed to me that FSS #2 was working on the special job"),

16 ("FSS #1 told me"), 18 (same), 36 (ER 68, 69, 72). Marcus's declaration is entirely dependent upon Klein's assertions and the documents he provided, as well as miscellaneous web sites. *E.g.*, SER 158. Klein's inadmissible evidence would be insufficient to defeat summary judgment in even a garden-variety case,[9] and with good reason: it would be impossible to cross-examine Klein meaningfully. The *only* thing Klein claims to know personally about the supposed "secret room" is that it allegedly contains "a storage cabinet" and "some poorly installed cable." Klein Decl. ¶ 17 (ER 69).

Moreover, the Klein and Marcus declarations fail to prove what Plaintiffs themselves say they need to allege and prove: "that AT&T acquired [their communications] for and disclosed [them] to the Government," Hepting Br. 61.[10] Contrary to Plaintiffs' rhetoric, these declarations have not "already established by

---

[9] *See Skillsky v. Lucky Stores, Inc.*, 893 F.2d 1088, 1091 (9th Cir. 1990); Fed. R. Civ. P. 56(e).

[10] Although beyond the scope of this brief, Plaintiffs' account of the elements of the various claims they raise, *see* Hepting Br. 88-90 (App.), is not accurate and wholly ignores the array of immunities and defenses potentially available to AT&T, which would have to be litigated and rejected before Plaintiffs could ever be entitled to judgment. *See, e.g.*, 18 U.S.C. §§ 2520(d), 2707(e) (good-faith defenses); *see also id.* §§ 2511(3)(a) (requiring proof that Plaintiffs' communications were divulged while in transmission), 2702(a)(1) (requiring proof that Plaintiffs' communications were in electronic storage at the time of disclosure); 47 U.S.C. § 605(a) (requiring proof that the communication was an interstate or foreign communication); 50 U.S.C. §§ 1801(f) (requiring proof that the interception occurred in the United States), 1805(i) (emergency exception to FISA).

unrebutted record evidence," *id.* at 62, 69, that AT&T disclosed any named plaintiff's communications to the government, and certainly not that AT&T "intercepted virtually all communications headed into and out of the [secret room]" and "divulged every single one of these communications to the NSA," *id.* at 63. At most, Klein and Marcus purport to establish the existence of a room, access to which is controlled by the NSA, into which some communications traffic is split, the infrastructure for which *could be* used for surveillance purposes. Klein and Marcus do not claim to know whether surveillance was actually conducted or whether communications were in fact divulged to the government,[11] much less can they say that a dragnet program of the kind Plaintiffs allege exists. Indeed, they do not even explain what happened in the supposed secret room. By Plaintiffs' own admission, Klein had no access to that room and entered it only "at one point, . . .

---

[11] Contrary to Plaintiffs' claims that it is irrelevant whether any human ever viewed the content of their communications, only those individuals whose communications were actually examined by the government could possibly have suffered concrete injury-in-fact sufficient to confer standing to challenge the claimed "search" or "divulgence" – something that no named plaintiff here could establish in light of the government's state secrets assertion. *See United States v. Karo*, 468 U.S. 705, 712 (1984) ("[W]e have never held that potential, as opposed to actual, invasions of privacy constitute searches for purposes of the Fourth Amendment."); Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 551-52 (2005); *cf.* Richard A. Posner, *Not a Suicide Pact: The Constitution in a Time of National Emergency* 97 (2006) ("Rather than invading privacy, computer sifting prevents most private data from being read by an intelligence officer or other human being by filtering them out.").

briefly." *Id.* at 5; SER 3-4. He places no NSA employee in that room at any time. Marcus surmises that the Internet configuration is "capable" of transmitting, or "ha[s] the capacity to" transmit, massive streams of data to the government, Marcus Decl. ¶¶ 38, 39, 44, 79 (ER 85, 87, 95), but neither he nor Klein knows whether any such thing occurred, *see also id.* ¶ 108 ("significant traffic to and from the plaintiffs . . . *would have been available for* interception") (ER 102) (emphasis added). Marcus admits that he does not know what happens to the signals that he surmises would be sent from the secret room. *Id.* ¶ 77 (ER 94). Neither Klein nor Marcus explains what information, if any, AT&T purportedly turned over to the NSA, under what circumstances, or why. Indeed, they do not claim – because they do not know – that *any* information was in fact turned over to the NSA, still less whether such information included Plaintiffs' communications. Plaintiffs' assertion (at 68) that these declarations establish to a "near certainty" that "AT&T has diverted their personal communications and records to the NSA" is thus at best wishful thinking utterly unsupported by the declarations themselves.

The questions raised but not resolved by these declarations make clear the case must be dismissed. Establishing standing would, at a minimum, require Plaintiffs to establish that AT&T disclosed *their* communications to the NSA, as

Plaintiffs repeatedly concede. Hepting Br. 52, 61, 62, 68.[12] It does not suffice to assert, even if Klein had done so, that all AT&T Internet traffic is routed to the "secret room." Without being able to litigate what went on in the supposed "secret room," it is impossible to know whether any such delivery occurred. There might have been no actual disclosure of information to the government at all. Even if one were to assume that some government-related activity was occurring in the room, the room could have been used for compliance with the Communications Assistance for Law Enforcement Act's requirement that telecommunications carriers possess infrastructure for sharing information with the government, *see* 47 U.S.C. § 1002(a), or for normal FISA surveillance.[13]

For all these reasons, Plaintiffs are mistaken that the parties need not "discover or prove the internal operations of [alleged] secret programs" for the litigation to proceed, Hepting Br. 51, and that the case is "straightforward" and requires "minimal" evidence, none of it secret, *id.* at 60-63, 88-90. On the contrary, this case is controlled by the numerous decisions like *El-Masri*, *Sterling*,

---

[12] Because even this most basic fact cannot be litigated without state secrets, to decide this case in AT&T's favor this Court need not decide what else Article III or statutory standing (or the substantive elements of Plaintiffs' claims) might require.

[13] That Marcus does not believe this to be the case, *see* Marcus Decl. ¶¶ 128-139 (ER 107-10), is beside the point, as there can be no adversarial testing of his opinion.

and *Zuckerbraun*, which recognize that litigation regarding the details of what are alleged to be classified intelligence or military activities is impossible. The Klein and Marcus declarations do nothing to change that.

C. Plaintiffs Cannot Establish Their Standing by Claiming Mere "Risk" of Injury

Finally, Plaintiffs' claim (at 77) that they 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" fails for multiple reasons. As a threshold matter, just as with the separate issue of whether AT&T participated in any alleged program, Plaintiffs cannot prove that they were or will be harmed by that program without knowing the details of the allegedly harmful conduct. In fact, this is even more so for claims of "likely" future harm, which necessarily require a fact-specific evaluation of whether the named plaintiffs are "immediately in danger of sustaining some direct injury." *City of Los Angeles v. Lyons*, 461 U.S. 95, 101-02 (1983) (internal quotation marks omitted). And the state secrets doctrine prevents them from discovering that information, if any exists, for the same reasons set forth above. This point alone is dispositive.

In any event, Plaintiffs offer no support for their claim that a likelihood of *past* injury is enough to establish standing. Hepting Br. 78; *accord* EPIC Br. 23. Each case they identify (at 78 & n.15) involved *actual past* injury or past conduct accompanied by *likely future* injury; not one holds that likely past injury is enough.

A claim that a plaintiff *might* have been harmed in the past neither provides the concrete, particularized injury-in-fact that Article III requires nor satisfies the specific statutory standing requirements that Plaintiffs show they "*were* subject to electronic surveillance," 50 U.S.C. § 1801(k) (emphasis added).[14]

The only cases in which a likelihood of harm has ever been held sufficient to confer standing involve a likelihood of *future* harm. These cases relate only to standing to seek *prospective* remedies. This is true of every case cited by Plaintiffs or their *amici*.[15] Thus, any claim of future harm could only support Plaintiffs' request for injunctive relief and not their damages claims. *See Lyons*, 461 U.S. at 109, 111.

But, even as to injunctions, the future harm exception to normal standing rules is a narrow one and does not apply here. As Plaintiffs recognize, this form of standing encompasses only "[c]ertain harms [that] are '"*by nature* probabilistic."'"

---

[14] *See also* 18 U.S.C. §§ 2520(a) (civil action for a "person whose . . . communication is intercepted, disclosed, or intentionally used"), 2707(a) (suit by "person aggrieved"), 2711(1) (adopting § 2510(11) definition of "aggrieved person"); 47 U.S.C. § 605(a), (e)(3)(A); *United States ex rel. Ross v. LaVallee*, 341 F.2d 823, 824 (2d Cir. 1965).

[15] *Covington v. Jefferson County*, 358 F.3d 626 (9th Cir. 2004), and *Helling v. McKinney*, 509 U.S. 25 (1993), are not future harm cases at all: in *Covington*, although the opinion speaks in terms of threats and risks, the case involved existing nuisance-type injuries to a landowner living next to a county dump, *see* 358 F.3d at 638 ("factual showing of fires, of excessive animals, insects and other scavengers . . . , and of groundwater contamination"), and *Helling* is not a standing case but rather an interpretation of the Eighth Amendment.

Hepting Br. 79 (emphasis added). The paradigm is environmental law, where "requir[ing] actual evidence of environmental harm, rather than an increased risk based on a violation of the statute, misunderstands the nature of environmental harm." *Central Delta Water Agency v. United States*, 306 F.3d 938, 948 (9th Cir. 2002) (internal quotation marks omitted). Outside the specific contexts of environmental harm (*Central Delta Water Agency*, *Covington*, *Friends of the Earth*, *Hall*, *Maine Peoples' Alliance*, *Mountain States Legal Foundation*), risks to human health (*Baur*, *Dimarzo*, *Harris*, *Helling*, *Sutton*), and challenges to administrative action or statutes, where standing naturally depends upon a prediction about how a challenged regulation or law might affect the plaintiff in the future (*American Library Association*, *Babbitt*, *Bryant*, *Churchill County*, *Hall*, *Simon*, *Teamsters*, *Village of Elk Grove*), *see* Hepting Br. 77-79; EPIC Br. 17-22, cases are few and far between.[16]

[16] Those few that exist, such as *Clinton v. City of New York*, 524 U.S. 417 (1998), and *United States v. Pawlinski*, 374 F.3d 536 (7th Cir. 2004), involved claims and facts so idiosyncratic they are not properly classed as future harm cases at all. *Clinton*, for example, involved a constitutional challenge by the City of New York to the line-item veto, where a farmers' cooperative's standing was based upon the fact that the President had *already* vetoed a line item that Congress had passed for its benefit. *See* 524 U.S. at 432. Likewise, *Pawlinski* was concerned with whether a convicted felon who had made restitution of the proceeds of his fraud retained enough of an interest in their ultimate disposition to be heard on that subject. *See* 374 F.3d at 538-39.

The injuries that flow from surveillance have never been understood to fall into the limited category of "probabilistic" harms that can support standing to seek to enjoin such activities by those who may not have been subject to them. On the contrary, the causes of action by their terms require actual, existing injury, *see supra* p. 27 & n.14; AT&T Br. 25 n.11, and standing in surveillance cases requires the plaintiff to present "proof of *actual acquisition* of [his] communications," *Halkin II*, 690 F.2d at 999-1000 (emphasis added); AT&T Br. 24-25.

The main case on which Plaintiffs rely – *LaDuke v. Nelson*, 762 F.2d 1318, 1322-26 (1985), *amended on other grounds*, 796 F.2d 309 (9th Cir. 1986), a Fourth Amendment case, proves the point. There, the Court's finding of likely *future* harm was predicated upon specific factual findings of a *past* injury that was likely to recur, as well as a determination of a pattern or practice of unlawful conduct taken against a certified class. *Id.* at 1324-25; *see Central Delta Water Agency*, 306 F.3d at 949 n.7 (recognizing the distinction between cases involving likely future harm and likely recurring harm). Such "pattern-and-practice" cases, which flow from *Lyons*, allow plaintiffs who have already been victimized to seek injunctions based on a credible threat of continuing unlawful behavior by the defendants. No such findings could be made here. Nothing has been established about what, if anything, AT&T actually did for the NSA, much less whether any such conduct was illegal or involved Plaintiffs. And the assertion of the state

secrets privilege means AT&T cannot defend itself against such allegations and, therefore, such allegations are not susceptible to judicial resolution. Under these circumstances, Plaintiffs cannot establish the predicate of past injury that would bring them into the *Lyons* and *LaDuke* line of cases, much less the details that would be necessary to show that they are "immediately in danger of sustaining some direct injury." *Lyons*, 461 U.S. at 101-02 (internal quotation marks omitted).

IV. SECTION 1806(f) OF FISA DOES NOT APPLY HERE, AND IN ANY EVENT DOES NOT DISPLACE THE CONSTITUTIONALLY ROOTED STATE SECRETS PRIVILEGE

Plaintiffs' final mistake is their reliance on § 1806(f). According to Plaintiffs, § 1806(f) permits litigation to proceed that otherwise could not, *see* Hepting Br. 27-29, 52; allows disclosures that are prohibited by the state secrets privilege, *id.* at 30; displaces *Totten*, *id.* at 48-49; justifies disregarding cases like *El-Masri*, *Zuckerbraun*, and *Sterling* that protect against disclosing operational details of classified programs, *id.* at 52; and even provides a special procedure for adjudicating standing where, as here, none could otherwise be established, *id.* at 81.

No court has ever employed § 1806(f) to overcome any of these hurdles, much less all of them, as would be necessary for Plaintiffs to prevail. There is simply no case law that supports *any* of Plaintiffs' arguments about its meaning or function. There are good reasons for that. Section 1806(f) does not apply to cases

like this one, and, even if it did, it serves a fundamentally different purpose from the state secrets doctrine. It certainly does not displace it.

A. Section 1806(f) Does Not Apply to This Case

Plaintiffs and their *amici* devote most of their energy to urging this Court to decide a weighty, constitutional question: whether Congress, in enacting § 1806(f), displaced the state secrets privilege. In their eagerness to reach that issue, Plaintiffs largely bypass the threshold question whether § 1806(f) even applies in these circumstances. It does not. Section 1806(f) is a tool for determining the legality of acknowledged surveillance. It *never* has been understood – not by any court, and not by Congress – as a tool for plaintiffs to discover *whether* they were surveilled. The text of § 1806(f) makes this clear.

Section 1806(f) applies only when two conditions have been satisfied. Neither has been met here. *First*, § 1806(f) applies only in cases involving an "aggrieved person," which FISA defines as "a person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance." 50 U.S.C. § 1801(k). As discussed above, Plaintiffs cannot show whether their communications were targeted or captured by the NSA. Plaintiffs have only their allegations, based on the limited observations of an AT&T employee with no security clearance, no access to the

details of any government surveillance program, and no relevant personal knowledge.

Plaintiffs argue (at 33) that such allegations are enough under § 1806(f). They are wrong. Their reading of the statute, which is not supported by any case, would allow a litigant capable of meeting the low standards of notice pleading to employ § 1806(f) to find out whether he was surveilled in what are alleged to be highly classified, ongoing intelligence programs. *Never* has § 1806(f) been understood to be a mechanism to allow parties to require the government to reveal whether they were subject to surveillance. In fact, the D.C. Circuit has rejected this argument. *See ACLU Found. v. Barr*, 952 F.2d 457, 468 & n.13 (D.C. Cir. 1991) ("[U]nder FISA, [the government] has no duty to reveal ongoing foreign intelligence surveillance.").

Instead, § 1806(f) is available to determine the legality of the surveillance of a *known* target, which typically occurs through a government admission. Indeed, in every reported case under § 1806(f), the government has acknowledged surveillance, and the question is whether the government can use the evidence gained from that admitted surveillance in a criminal or immigration proceeding. *See, e.g., United States v. Ott*, 827 F.2d 473, 475 n.1 (9th Cir. 1987) ("Because Ott's communications were subject to surveillance, he is an aggrieved person with standing to bring a motion to suppress pursuant to section 1806(e)."); *United States*

v. Cavanagh, 807 F.2d 787, 789 (9th Cir. 1987) ("Appellant was a party to an intercepted communication, and the government concedes he is an 'aggrieved person' within the meaning of the statute. The appellant has standing to challenge the government's compliance with [FISA].") (citation omitted); *see also United States v. Damrah*, 412 F.3d 618, 625 (6th Cir. 2005) (immigration proceeding); *United States v. Johnson*, 952 F.2d 565, 573 (1st Cir. 1991) (criminal proceeding); *United States v. Isa*, 923 F.2d 1300, 1305-06 (8th Cir. 1991) (criminal proceeding).

The text and structure of § 1806 likewise confirm that § 1806(f) is not a tool for determining whether a party was ever surveilled. Section 1806 expressly contemplates notification of targets under certain circumstances – namely, if the government intends to use information derived from surveillance against the target. 50 U.S.C. § 1806(c)-(d). That notice triggers a process under which that individual, an "aggrieved person," may challenge the legality of the surveillance and seek to suppress resulting evidence. *Id.* § 1806(e), (g). Section 1806(f) then comes into play when the government believes it necessary for the resulting suppression proceeding to be conducted *ex parte* and *in camera* in federal court. *Id.* § 1806(f). Nothing about this process suggests that it is intended as a tool for private persons to explore a suspicion that they are under surveillance. Indeed, the existence of the limited notification requirements in subsections 1806(c), (d), and (j) indicates that FISA does not impose broader notification requirements on the

government, through § 1806(f) or otherwise. *See Barr*, 952 F.2d at 468 n.13; *see also O'Melveny & Myers v. FDIC*, 512 U.S. 79, 86 (1994) ("*Inclusio unius, exclusio alterius.*"). And in the context of the only disclosure requirement in § 1806 that is *not* tied to offensive use of evidence by the government – the requirement in § 1806(j) of disclosure to the target of certain forms of emergency surveillance – Congress expressly recognized that notice could be forgone for "good cause." The legislative history confirms that, "if the Government can show a likelihood that notice would compromise an ongoing investigation, or confidential sources or methods, *notice should not be given.*" S. Rep. No. 95-604, pt. 1, at 60 (1978) (emphasis added), *reprinted in* 1978 U.S.C.C.A.N. 3904, 3961. This cuts directly against the notion that § 1806(f) is an all-purpose tool for having the courts force the government to come forward and confirm or deny whether it is conducting surveillance of particular individuals.

If Plaintiffs' proposed interpretation of § 1806(f) were correct, then the first step for the district court would be to determine, through § 1806(f), whether the named Plaintiffs are aggrieved – *i.e.*, whether they have standing. But, no matter how carefully the district court proceeded, it could not avoid disclosing sensitive information about the targeting of alleged intelligence-gathering activities. Even in the absence of any explanation or findings by the court, if the case were allowed to proceed, Plaintiffs, and the world, would know that their communications had been

intercepted; if not, they would know the opposite. Thus, the very process of determining whether Plaintiffs are "aggrieved persons" for these purposes would reveal information that the Director of National Intelligence has stated must remain secret to avoid grave danger to national security. That result is directly contrary to the congressional intent behind § 1806(f) and related notice provisions, which are intended to preserve the Executive's ability to prevent public disclosure of sensitive information.

Second, far from creating a tool to allow private parties to determine whether they were surveilled, Congress made it the *government's* sole prerogative to invoke the § 1806(f) procedure, which has not occurred here. By its terms, § 1806(f) applies only "*if* the Attorney General 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) (emphasis added). Congress went so far as to define "Attorney General" in the statute, so that there could be no ambiguity about whether this condition had been satisfied. *Id.* § 1801(g). But the Attorney General has not invoked § 1806(f). Undeterred, Plaintiffs baldly assert (at 27) that this requirement was met by the filing of the declarations of the Director of National Intelligence for the separate purpose of asserting the state secrets privilege, but they offer no explanation how a state secrets assertion by the Director of National Intelligence to *prevent* litigation of standing could be transformed into an affidavit by the

Attorney General invoking § 1806(f) to *permit* such litigation, especially where the Attorney General himself is arguing strenuously against the application of § 1806(f). Plaintiffs' *amici* are somewhat more forthright in acknowledging the problem, but offer no solution. They claim that "the government has refused to invoke" § 1806(f), Chemerinsky Br. 11-12, as though this were somehow a requirement, notwithstanding the statute's use of the word "if," which plainly indicates that this is a matter of choice for the government.

B. The State Secrets Privilege Is Not Displaced by FISA

In any event, even if § 1806(f) applied here, Plaintiffs still could not employ it to defeat the government's state secrets motion unless they could meet the heavy burden of demonstrating that FISA wholly displaced, *sub silentio*, the state secrets privilege. They cannot. A statute that is claimed to invade the common law must "'be read with a presumption favoring the retention of long-established and familiar principles, except when a statutory purpose to the contrary is *evident*.'" *Kasza*, 133 F.3d at 1167-68 (quoting *United States v. Texas*, 507 U.S. 529, 534 (1993)) (emphasis added). Plaintiffs' burden is all the greater here because the state secrets privilege is an aspect of executive privilege rooted in the constitutional separation of powers.[17] Because a statutory abrogation of the state

---

[17] *See El-Masri*, 479 F.3d at 304 ("The state secrets privilege that the United States has interposed in this civil proceeding . . . has a firm foundation in the

secrets doctrine would raise serious constitutional questions, Congress would need to speak clearly on this point if it wished the courts to confront these questions. *See INS v. St. Cyr*, 533 U.S. 289, 299-300 (2001); *Reynolds*, 345 U.S. at 6 (declining to find that "the executive's power to withhold documents was waived by" a federal statute because the privilege had "constitutional overtones").

Far from containing a clear statement of intention on this point, FISA contains *no* indication that Congress meant to displace this privilege. Plaintiffs cannot identify a single place in which anyone associated with the passage of FISA ever suggested that the statute would displace the state secrets doctrine. Nothing in the statute. Nothing in the legislative history. Not even a single floor statement by a member of Congress. And certainly no case law from the intervening 30 years. Nothing.

Thus, Plaintiffs and their *amici* fall back on broad claims about the statute's supposed purpose, and from that infer that Congress must have displaced the state secrets privilege. Hepting Br. 30-32; PFAW Br. 13-18; Chemerinsky Br. 6-10. But neither FISA's purpose nor its provisions are inconsistent with the state secrets privilege. The purpose of the state secrets privilege is to "protect[] military and

---

Constitution, in addition to its basis in the common law of evidence."); *see also United States v. Nixon*, 418 U.S. 683, 710 (1974); *Department of the Navy v. Egan*, 484 U.S. 518, 527 (1988).

state secrets." *Reynolds*, 345 U.S. at 7. Section 1806(f), on the other hand, does not require the court to evaluate whether disclosure will harm national security. Instead, it focuses on the very different question whether surveillance was "lawfully authorized and conducted."

Far from intending to displace the government's ability to protect state secrets, as Plaintiffs assert (*e.g.*, at 28), Congress broadly understood that "[b]y its very nature foreign intelligence surveillance must be conducted in secret. [FISA] reflects the need for such secrecy; judicial review is limited to a select panel and *routine notice to the target is avoided*." S. Rep. No. 95-604, pt. 1, at 60, *reprinted in* 1978 U.S.C.C.A.N. 3962 (emphasis added). And, in the specific context of § 1806(f), Congress understood that the ultimate decision whether to reveal secret information was a *separate* one that must remain with the nation's intelligence officials: if the United States concludes that disclosing surveillance-related information would "damage the national security," it can ordinarily "either disclose the material or forgo use of the surveillance-based evidence." S. Rep. No. 95-701, at 65, *reprinted in* 1978 U.S.C.C.A.N. 4034; *accord* S. Rep. No. 95-604, pt. 1, at 58, *reprinted in* 1978 U.S.C.C.A.N. 3960.

Finally, Plaintiffs mistakenly suggest (at 27) that applying the state secrets privilege to FISA claims would render the cause of action under that statute a nullity. But this is a *non sequitur* – the fact that Congress creates a cause of action

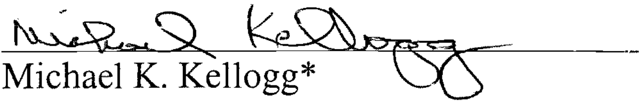
does not mean that no legal doctrine, privilege, or immunity can defeat that cause of action in a particular case. Indeed, the state secrets privilege has repeatedly been held to apply in suits based upon express rights of action, including *Reynolds* itself. *See* 345 U.S. at 2 (suit under the Federal Tort Claims Act); *see also*, *e.g.*, *Kasza*, 133 F.3d at 1162 (citizen-suit under Resource Conservation and Recovery Act of 1976). Plaintiffs' view is also utterly incompatible with decisions holding that statutory disclosure mechanisms – even, for instance, those in FOIA that relate specifically to national security – do not displace the traditional and constitutionally rooted state secrets privilege.[18]

CONCLUSION

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

[18] *See, e.g., EPA v. Mink*, 410 U.S. 73, 87-88 (1973), *superseded by statute on other grounds as recognized in Zweibon v. Mitchell*, 516 F.2d 594, 642 (D.C. Cir. 1975) (en banc); *Baker & Hostetler LLP v. United States Dep't of Commerce*, 473 F.3d 312 (D.C. Cir. 2006).

Respectfully submitted,



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

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

*Counsel of Record

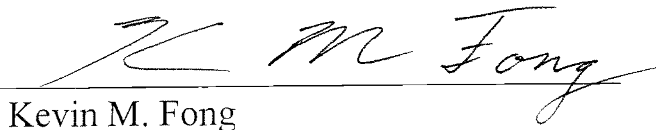
David W. Carpenter
Bradford A. Berenson
Edward R. McNicholas
Eric A. Shumsky
SIDLEY AUSTIN LLP
1501 K Street, N.W.
Washington, D.C. 20005
(202) 736-8000

May 24, 2007

CERTIFICATE OF COMPLIANCE PURSUANT TO FEDERAL RULE OF APPELLATE PROCEDURE 32(a)(7)(C) AND NINTH CIRCUIT RULE 32-1 FOR CASE NO. 06-17132

I certify, pursuant to Federal Rule of Appellate Procedure 32(a)(7)(C) and Ninth Circuit Rule 32-1, that the foregoing brief is proportionately spaced, has a typeface of 14 points, and contains 9,691 words. AT&T is contemporaneously filing with this Court a Motion To File an Enlarged Reply Brief of this number of words.

May 24, 2007



Kevin M. Fong

Docket No. 06-17132

PROOF OF SERVICE BY MAIL

I, Jan Molitor, the undersigned, hereby declare as follows:

1. I am over the age of 18 years and am not a party to the within cause. I am employed by Pillsbury Winthrop Shaw Pittman LLP in the City of San Francisco, California.

2. My business address is 50 Fremont Street, San Francisco, CA 94105-2228. My mailing address is 50 Fremont Street, P. O. Box 7880, San Francisco, CA 94120-7880.

3. I am familiar with Pillsbury Winthrop Shaw Pittman LLP's practice for collection and processing of correspondence for mailing with the United States Postal Service; in the ordinary course of business, correspondence placed in interoffice mail is deposited with the United States Postal Service with first class postage thereon fully prepaid on the same day it is placed for collection and mailing.

4. On May 24, 2007, at 50 Fremont Street, San Francisco, California, I served true copies of the attached document titled exactly REPLY BRIEF OF APPELLANT AT&T CORP. by placing them in an addressed, sealed envelopes clearly labeled to identify the persons being served at the addresses shown below and placed in interoffice mail for collection and deposit in the United States Postal Service on that date following ordinary business practices:

[See Attached Service List]

I declare under penalty of perjury that the foregoing is true and correct. Executed this 24th day of May, 2007, at San Francisco, California.

____

Jan Molitor

No. 06-17132
MAILING LIST

Cindy Ann Cohn
Lee Tien
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110

Bert Voorhees
Traber, Voorhees & Olguin
128 North Fair Oaks Avenue
Suite 204
Pasadena, CA 91103

Eric B. Fastiff
Barry R. Himmelstein
Lieff, Cabraser, Heimann & Bernstein, LLP
275 Battery Street
30th Floor
San Francisco, CA 94111

James S. Tyre
10736 Jefferson Blvd.
512
Culver City, CA 90230

Richard R. Wiebe
Law Office of Richard R. Wiebe
425 California Street
Suite 2025
San Francisco, CA 94104

Jeffrey Friedman
Hagens Berman Sobel Shapiro LLP
425 Second Street
Suite 500
San Francisco, CA 94107

Elena M. DiMuzio
E. Joshua Rosenkranz
Heller Ehrman LLP
333 Bush Street
San Francisco, CA 94104

Eric A. Isaacson
Lerach Coughlin Stoia Geller
Rudman & Robbins LLP
655 West Broadway
Suite 1900
San Diego, CA 92101-3301

Aram Antaramian
Law Office of Aram Antaramian
1714 Blake Street
Berkeley, CA 94703

Attorneys for Tash Hepting, et al.,
Plaintiffs-Appellees

Lisa R. Jaskol
610 S. Ardmore Avenue
Los Angeles, CA 90005

Jon B. Eisenberg
Eisenberg and Hancock, LLP
1970 Broadway
Suite 1200
Oakland, CA 94612

Steven Goldberg
River Park Center, Suite 300
205 SE Spokane Street
Portland, OR 97202

J. Ashlee Albies
Law Offices of J. Ashlee Albies
205 SE Spokane Street
Portland, OR 97202

Thomas H. Nelson
Thomas H. Nelson & Associates
24525 E. Welches Road
P.O. Box 1211
Welches, OR 97067

Attorneys for Al-Haramain Islamic Foundation, et al., Plaintiffs-Appellees in Consolidated Docket No. 06-36083

Peter D. Keisler
Anthony J. Coppolino
Andrew H. Tannenbaum
U.S. Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Avenue, NW
Room 6102
Washington, DC 20001

Douglas N. Letter
Thomas M. Bondy
Anthony A. Yang
U.S. Department of Justice
Civil Division, Appellate Staff
950 Pennsylvania Avenue, N.W.
Room 7513
Washington, DC 20530

Paul D. Clement
Gregory G. Garre
Daryl Joseffer
U.S. Department of Justice
Office of the Solicitor General
950 Pennsylvania Avenue, N.W.
Room 5614
Washington, DC 20530

Attorneys for George W. Bush and United States of America, Defendants-Intervenors

Timothy L. Alger
Quinn Emanuel Urquhart
Oliver & Hedges, LLP
865 S. Figueroa Street
10th Floor
Los Angeles, CA 90017-2543

Attorney for Intervenors Wired News and Condenet, Inc. (Amici)

Jennifer Stisa Granick
Stanford Law School Legal Clinics
Crown Quadrangle
559 Nathan Abbott Way
Stanford, CA 94305-8610

Attorney for Professor Susan Freiwald, (Amicus)

Terry Gross
Gross & Belsky LLP
180 Montgomery Street
Suite 220
San Francisco, CA 94104

Attorney for The Center for National Security Studies (Amicus)

Roger R. Myers
Holme Roberts & Owen, LLP
560 Mission Street
25th Floor
San Francisco, CA 94105

Attorney for The California First Amendment Coalition, CNET News.com (Amici)

Jonathan Banks
United States Telecom Association
607 14th Street, NW
Suite 400
Washington, DC 20005

Andrew G. McBride
Wiley Rein LLP
1776 K Street, NW
Washington, DC 20006

Attorneys for United States Telecom Association (Amicus)

John A. Rogovin
Wilmer Cutler Pickering Hale & Dorr LLP
1875 Pennsylvania Avenue, NW
Washington, DC 20006-3642

Henry Weissman
Munger, Tooles & Olson LLP
355 South Grand Avenue
35th Floor
Los Angeles, CA 90071-1560

Attorneys for Verizon Communications, Inc. (Amicus)

Lawrence S. Ebner
McKenna Long & Aldridge, LLP
1900 K Street, NW
Washington, DC 20006

Robin S. Conrad
Amar D. Sarwal
National Chamber Litigation Center, Inc.
1615 H Street, NW
Washington, DC 20062

Attorneys for Chamber of Commerce of the United States (Amicus)

Lauren Gelman
Cyberlaw Clinic
Center for Internet and Society
Stanford Law School
Crown Quadrangle
559 Nathan Abbott Way
Stanford, CA 94305-8610

Attorney for Consumer Rights Groups, Center for Digital Democracy, Consumer Federation of America, Consumers Union, PrivacyActivism and U.S. Public Interest Research Group, (Amici)

Gary L. Bostwick
Jean-Paul Jassy
Bostwick & Jassy LLP
12400 Wilshire Boulevard
Suite 400
Los Angeles, CA 90025

Attorney for Professors Robert M. Pallitto, William G. Weaver (Amici)

Heidi Kitrosser
Associate Professor
University of Minnesota Law School
229-19th Avenue South
Minneapolis, MN 55455

Stephen I. Vladeck
Associate Professor
University of Miami School of Law
1311 Miler Drive
Coral Gables, FL 33146

Attorneys for Erwin Chemerinsky et al., Law Professors (Amici)

Jonathan M. Freiman
Yale Law School
P.O. Box 208215
New Haven, CT 06520-8215

Attorney for National Security Archive, Project on Government Oversight, Project on Government Secrecy, Public Citizen, Inc. and The Rutherford Institute (Amici)

Judith E. Schaeffer
People for the American Way Foundation
2000 M Street, NW
Suite 400
Washington, DC 20036

Jack Lerner
University of California at
Berkeley School of Law
Boalt Hall
396 Simon Hall
Berkeley, CA 94720-7200

Attorneys for People for the American Way Foundation (Amicus)

Kathleen M. Sullivan
Constitutional Law Center
Stanford Law School
559 Nathan Abbott Way
Stanford, CA 94305-8610

Attorney for Electronic Privacy Information Center, Center for Democracy and Technology, and Computer Scientists for Professional Responsibility (Amici)

Sidney S. Rosdeitcher
Chair, Committee on Civil Rights
The Association of the Bar of the
City of New York
1285 Avenue of Americas
New York, NY 10019-6064

Peter T. Barbur
Cravath Swaine & Moore LLP
Worldwide Plaza
825 Eighth Avenue
New York, NY 10019

Attorneys for The Association of the Bar of the City of New York, The Bar Association of San Francisco, The Beverly Hills Bar Association, The Chicago Bar Association and The Los Angeles Bar Association (Amici)

Adam H. Charnes
Kilpatrick Stockton LLP
1001 West Fourth Street
Winston-Salem, NC 27101

Attorney for Professor Robert M. Chesney (Amicus)

Marc Van der Hout
Van der Hout, Brigagliano & Nightingale, LLP
180 Sutter Street
5th Floor
San Francisco, CA 94104-4029

Jonathan Hafetz
Brennan Center for Justice at
NYU School of Law
161 Avenue of the Americas
12th Floor
New York, NY 10013

Attorneys for National Association for the Advancement of Colored People, American-Arab Anti-Discrimination Committee, Asian American Legal Defense and Education Fund, Japanese American Citizens League, The League of United Latin American Citizens and United for Peace and Justice (Amici)