

Exhibit B

Ilann M. Maazel
Matthew D. Brinckerhoff
Kennisha Austin
Emery Celli Brinckerhoff & Abady LLP
75 Rockefeller Plaza, 20th Floor
New York, New York 10019
Telephone: (212) 763-5000
Facsimile: (212) 763-5001
Attorneys for Plaintiffs

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA**

IN RE NATIONAL SECURITY AGENCY)
TELECOMMUNICATIONS RECORDS)
LITIGATION)

MDL Dkt. No. 06-1791-VRW

This Document Relates to:)

**PLAINTIFFS' MEMORANDUM
OF LAW IN OPPOSITION TO
MOTION TO DISMISS OR FOR
SUMMARY JUDGMENT BY
THE UNITED STATES AND
THE OFFICIAL CAPACITY
DEFENDANTS**

VIRGINIA SHUBERT, NOHA ARAFA,)
SARAH DRANOFF and HILARY)
BOTEIN, individually and on behalf of all)
others similarly situated,)

Plaintiffs,)

-against -)

Date: August 30, 2007
Time: 2:00 pm
Courtroom: 6
Hon. Vaughn R. Walker

GEORGE W. BUSH, MICHAEL V.)
HAYDEN, KEITH B. ALEXANDER,)
ALBERTO GONZALES, JOHN)
ASHCROFT, UNITED STATES OF)
AMERICA, and JOHN/JANE)
DOES #1-100 (07-693))

-----)

TABLE OF CONTENTS

PAGE NO(s):

TABLE OF AUTHORITIES iv-xi

PRELIMINARY STATEMENT 1

FACTS 3

ARGUMENT 5

 I. The Complaint States a Claim for Violation of the Fourth
 Amendment and FISA 5

 A. The Complaint Alleges Violations of FISA 5

 B. The Complaint Alleges Violations of the Fourth Amendment 10

 1. The Dragnet is Warrantless 10

 2. The Dragnet is General and Indiscriminate, Not Specific
 and Particularized 15

 3. The Dragnet is Not Reasonable Or Based Upon Probable
 Cause 16

 II. The Executive’s Radical Extension of the State Secrets Privilege
 Cannot Bar This Suit 17

 A. FISA Itself Precludes Application of the State Secrets
 Privilege In This Case 17

 1. The FISA Cause of Action is Inconsistent With the
 State Secrets Privilege 18

 2. In Addition to Creating a Cause of Action, Congress
 Set Forth Specific Procedures to Govern Confidential
 Information Relating to Electronic Surveillance 20

 3. FISA Also Contemplated Discovery From
 Telecommunications Carriers 21

4.	FISA Precludes Dismissal	22
B.	Origins of the State Secrets Privilege and Constitutional Principles At Stake	23
1.	Principles of Separation of Powers	24
2.	The State Secrets Privilege	28
(i)	The Ninth Circuit and the State Secrets Privilege	33
(ii)	Other Circuits and the State Secrets Privilege	34
C.	The State Secrets Privilege Does Not Apply to a Massive, Illegal Program That Reaches Into the Heartland of This Country and Violates The Constitutional Rights of Millions of Ordinary Americans	36
1.	Because This Case Concerns Civilian, not “Military Matters,” the State Secrets Privilege Does Not Apply	37
2.	The Supreme Court Case in <i>Webster</i> Requires Balancing of the Parties’ Interests, not Dismissal	39
3.	<i>Reynolds</i> , Which Was Decided In a Considerably Different Factual Context, Does Not Require Dismissal	42
4.	Because the Content Monitoring Program Is Not Secret, It Is Not a “State Secret”	45
D.	The <i>Totten/Tenet</i> Bar Does Not Apply	46
III.	Defendants’ Standing Argument Is a Red Herring	47
A.	The Sixth Circuit Opinion in <i>ACLU v. NSA</i> Does Not Help Defendants	50
IV.	Defendants’ Statutory Arguments Fail	54
A.	Neither Statute Requires Dismissal	54
B.	FISA Supplants the Statutory Provisions	55

C.	On Its Face, Section 102(a)(i)(1) Applies to the DNI, Not to the Court	56
D.	The Statutes Plainly Do Not Preclude Discovery From Third-Parties	57
E.	Defendants' Interpretation of the Statutes Raises Serious Constitutional Concerns	57
CONCLUSION		59

TABLE OF AUTHORITIES

<u>CASES</u>	<u>PAGE NO(s)</u>
<i>ACLU Found. of Southern Cal. v. Barr</i> , 952 F.2d 457 (D.C. Cir. 1991)	22, 50-53
<i>Adams v. City of Battle Creek</i> , 250 F.3d 980 (6th Cir. 2001)	54
<i>Al-Haramain Islamic Found. v. Bush</i> , 451 F.Supp.2d 1215 (D.Or. 2006)	<i>passim</i>
<i>Al-Marri v. Wright</i> , 2007 WL 1663712 (4th Cir. June 11, 2007)	27, 38, 43-45
<i>American Civil Liberties Union v. National Security Agency</i> , 2007 WL 1952370 (6th Cir. July 6, 2007)	9, 48-50
<i>Bareford v. General Dynamics Corp.</i> , 973 F.2d 1138 (5th Cir. 1992)	37
<i>Berger v. New York</i> , 388 U.S. 41 (1967)	2, 10, 11, 15, 16
<i>Brinegar v. United States</i> , 338 U.S. 160 (1949)	3
<i>Busic v. United States</i> , 446 U.S. 398 (1980)	55, 56
<i>Chimel v. California</i> , 395 U.S. 752 (1969)	11, 15
<i>CIA v. Sims</i> , 471 U.S. 159 (1985)	56, 57
<i>City of Los Angeles v. Lyons</i> , 461 U.S. 95 (1983)	52
<i>Department of Navy v. Egan</i> , 484 U.S. 518 (1988)	37

Dickerson v. United States,
 530 U.S. 428 (2000) 17

Director, Office of Workers' Comp. Programs v. Newport News Shipbuilding & Dry Dock Co.,
 514 U.S. 122 (1995) 49

Edmonds v. United States Dept. of Justice,
 323 F.Supp.2d 65 (D.D.C. 2004) 37

Ellsberg v. Mitchell,
 709 F.2d 51 (D.C. Cir. 1983). 35, 36

El-Masri v. Tenet,
 479 F.3d 296 (4th Cir. 2007) 41

Ex Parte Milligan,
 71 U.S. 2 (1866) 25

Farnsworth Cannon, Inc. v. Grimes,
 635 F.2d 268 (4th Cir. 1980) 37

FEC v. Akins,
 524 U.S. 11 (1998) 49

Fitzgerald v. Penthouse Int'l, Ltd.,
 776 F.2d 1236 (4th Cir. 1985) 37

Fitzgibbon v. CIA,
 911 F.2d 755 (D.C. Cir. 1990) 56

Food & Drug Admin. v. Brown & Williamson Tobacco Corp.,
 529 U.S. 120 (2000) 55

Founding Church of Scientology v. NSA,
 610 F.2d 824 (D.C. Cir. 1979) 55, 57

Halkin v. Helms,
 598 F.2d 1 (D.C. Cir. 1978) 34-36

Halkin v. Helms,
 690 F.2d 977 (D.C. Cir. 1982) 34-36

Halpern v. United States,
 258 F.2d 36 (2nd Cir. 1958) 17-19, 23, 31, 34, 36, 41

Hamdan v. Rumsfeld,
 126 S.Ct. 2749 (2006) 18, 24

Hamdi v. Rumsfeld,
 542 U.S. 507 (2004) 18, 25

Hayden v. NSA,
 608 F.2d 1381 (D.C. Cir. 1979) 57

Hilao v. Estate of Marcos,
 103 F.3d 767 (9th Cir. 1996) 53

In re Under Seal,
 945 F.2d 1285 (4th Cir. 1991) 37

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

Jencks v. United States,
 353 U.S. 657 (1957) 45

Kasza v. Browner,
 133 F.3d 1159 (9th Cir. 1998) 17, 18, 23, 33, 34, 37, 40, 42

Katz v. United States,
 389 U.S. 347 (1967) 10, 11

Laird v. Tatum,
 408 U.S. 1 (1972) 27, 33, 43

Lujan v. Defenders of Wildlife,
 504 U.S. 555 (1992) 47, 51

Marbury v. Madison,
 5 U.S. 137 (1803) 1, 24, 39, 44

McDonald v. United States,
 335 U.S. 451 (1948) 11

Military Audit Project v. Casey,
 656 F.2d 724 (D.C. Cir. 1981) 37

Molerio v. FBI,
 749 F.2d 815 (D.C. Cir. 1984) 37

Multi Denominational Ministry v. Gonzales,
 474 F.Supp.2d 1133 (N.D.Cal. 2007) 53-54

Northrop Corp. v. McDonnell Douglas Corp.,
 751 F.2d 395 (D.C. Cir. 1984) 37

Organizacion JD Ltda v. U.S. Dept. Of Justice,
 18 F.3d 91 (2nd Cir. 1994) 54

Panetti v. Quarterman,
 127 S.Ct. 2842 (2007) 50

Payton v. New York,
 445 U.S. 573 (1980) 11

People for the Am. Way Found. v. NSA,
 462 F.Supp.2d 21 (D.D.C. 2006) 57

R.J. Reynolds Tobacco Co. v. Shewry,
 423 F.3d 906 (9th Cir. 2005) 3

Ramadan v. Gonzales,
 479 F.3d 646 (9th Cir. 2007) 58

Reid v. Covert,
 354 U.S. 1 (1957) 24, 27, 39

Retlaw Broadcasting Co. v. N.L.R.B.,
 53 F.3d 1002 (9th Cir. 1995) 53

Rochon v. Gonzales,
 438 F.3d 1211 (D.C. Cir. 2006) 54

Salazar v. Heckler,
 787 F.2d 527 (10th Cir. 1986) 54

Snepp v. United States,
 444 U.S. 507 (1980) 56

Stehney v. Perry,
 101 F.3d 925 (3rd Cir. 1996) 41

Sterling v. Tenet,
 416 F.3d 338 (4th Cir. 2005) 37

Tenet v. Doe,
 544 U.S. 1 (2005) 17-18, 23, 26, 29, 33, 37, 42, 47

Terkel v. AT&T Corp.,
 441 F.Supp.2d 899 (N.D.Ill. 2006) 56-58

The Presbyterian Church (U.S.A.) v. United States,
 870 F.2d 518 (9th Cir. 1989) 52

Tilden v. Tenet,
 140 F.Supp.2d 623 (E.D.Va. 2000) 37

TMJ, Inc. v. Nippon Trust Bank,
 2001 WL 925622 (9th Cir. Aug. 15, 2001) 5

Toth v. Quarles,
 350 U.S. 11 (1955) 27

Totten v. United States,
 92 U.S. 105 (1875) 18, 28, 29, 31, 33, 42, 46, 47

United States v. Belfield,
 692 F.2d 141 (D.C. Cir. 1982) 5

United States v. Burr,
 25 F.Cas. 30 (C.C.D.Va. 1807) 28

United States v. Karo,
 468 U.S. 705 (1984) 11

United States v. Nixon,
 418 U.S. 683 (1974) 18

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

United States v. United States District Court for the Eastern District of Michigan,
 689 U.S. 297 (1972) 5, 11, 13, 16

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

Wilbur v. Locke,
 423 F.3d 1101 (9th Cir. 2005) 3, 47

Youngstown Sheet & Tube Co. v. Sawyer,
 343 U.S. 579 (1952) *passim*

Zuckerbraun v. General Dynamics Corp.,
 935 F.2d 544 (2nd Cir. 1991) 37

Zweibon v. Mitchell,
 516 F.2d 594 (D.C. Cir. 1975) 13-15, 24

STATUTES

18 U.S.C. § 2510 6

18 U.S.C. § 2511(2)(a)(ii) 21-22

18 U.S.C. § 2511(2)(a)(ii) (1970) 21

18 U.S.C. § 2511(2)(f) 6

18 U.S.C. § 2520 21, 54

18 U.S.C. § 2522 6

18 U.S.C. § 2707(a) 54

35 U.S.C. § 181 *et seq.* 19

42 U.S.C. § 2000e-16(c) 54

50 U.S.C. § 402 54, 55

50 U.S.C. § 403-1(i)(1)	54
50 U.S.C. § 1801 <i>et seq.</i>	1, 53
50 U.S.C. § 1801(f)	7, 20
50 U.S.C. § 1801(k)	8
50 U.S.C. § 1801(m)	53
50 U.S.C. § 1805(a)(3)	8, 16
50 U.S.C. § 1805(f)	7
50 U.S.C. § 1806(f)	19-22, 56, 57
50 U.S.C. § 1809	8, 48, 53
50 U.S.C. § 1810	8, 48
50 U.S.C. § 1811	7
Pub. L. No. 90-351, 83 Stat. 311 (1968)	6
Pub. L. No. 107-40, 115 Stat. 224 (Sept. 18, 2001)	9
U.S. Const. amend. IV	<i>passim</i>

RULES

Fed. R. Civ. P. 12(b)(1) 5

Fed. R. Civ. P. 12(b)(6) 5

Fed. R. Civ. P. 56(f) 5

LEGISLATIVE MATERIALS

H.R. Conf. Rep. No. 95-1720 (1978), *reprinted in* 1978 U.S.C.C.A.N. 4048 6

S. Rep. No. 95-604(I) (1978), *reprinted in* 1978 U.S.C.C.A.N. 3904 5-9, 21

S. Rep. No. 95-701 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3973 6, 12, 14

S. Rep. No. 95-755 (1976) 5

S. Select Comm. To Study Governmental Operations with Respect to Intelligence Activities
 (Church Committee Books I-VI), available at
<http://www.aarclibrary.org/publib/church/reports/contents.htm> 5

PRELIMINARY STATEMENT

Defendants had a choice. After 9/11, defendants could have proposed a statute to amend FISA.¹ They could have proposed a constitutional amendment to limit or eliminate the Fourth Amendment in the foreign intelligence context. Instead they secretly violated FISA and the Fourth Amendment by instituting a massive, criminal, domestic spying program that monitors millions of telephone and internet communications of ordinary Americans. Now they seek to transform a limited, common law evidentiary privilege into a sweeping immunity for their own unlawful conduct. That they cannot do.

“With all its defects, delays and inconveniences, men have discovered no technique for long preserving free government except that the Executive be under the law.”² Defendants’ radical extension of the state secrets privilege flies in the face of over two centuries of American jurisprudence: law that established the constitutional right and duty of Article III courts to “say what the law is,” *Marbury v. Madison*, 5 U.S. 137, 177 (1803); the right to be free from unreasonable searches and seizures, *see* U.S. Const. amend. IV; the right to a judicial forum to assert constitutional rights, *see Webster v. Doe*, 486 U.S. 592 (1988); and constitutional limitations upon Executive power, *see Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579 (1952).

Defendants would sweep away these vital constitutional principles with the stroke of a declaration, arrogating to themselves the right to immunize *any* criminal or unconstitutional

¹The Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801 *et seq.*

²*Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 655 (1952) (Jackson, J., concurring).

conduct in the name of national security. Defendants cannot so easily puncture a hole in the Constitution. The motion should be denied because:

- FISA preempts the state secrets privilege, setting forth a reasoned mechanism balancing national security interests with plaintiffs' FISA rights and the Court's obligation to uphold the law (*see infra* Point II(A));
- The state secrets privilege, by its own terms, does not apply to a massive domestic spying program targeted at millions of ordinary Americans (*see infra* Point II(C)(1));
- The Supreme Court case in *Webster v. Doe*, 486 U.S. 592 (1988), which post-dates *United States v. Reynolds*, 345 U.S. 1 (1953), compels balancing of the parties' interests, not dismissal (*see infra* Point II(C)(2));
- *Reynolds*, which arose in a considerably different factual context, plainly does not compel dismissal (*see infra* Point II(C)(3));
- Defendants' surveillance program is not even a secret, much less a "state secret" (*see infra* Point II(C)(4));
- Defendants' standing argument falls with their state secrets argument (*see infra* Point III); and
- Defendants' half-hearted statutory arguments also fail (*see infra* Point IV).

The Executive has illegally placed the intelligence arm of the United States military "in the bedroom, in the business conference, in the social hour, in the lawyer's office—everywhere and anywhere a 'bug' can be placed."³ But defendants' motion is even more frightening than the conduct alleged in the Amended Complaint. For defendants offer no limiting principle for their radical argument. In defendants' view, a secret program by the Executive to put a camera in every American's bedroom could not be revealed, if to reveal it might harm national security. A secret program by the Executive to abduct and torture

³*Berger v. New York*, 388 U.S. 41, 64-65 (1967) (Douglas, J., concurring).

Americans could not be revealed, challenged, much less enjoined, if to reveal it might harm national security.

Article III courts exist to prevent such unchecked power. “Uncontrolled search and seizure is one of the first and most effective weapons in the arsenal of every arbitrary government.”⁴ So too the uncontrolled ability of the Executive to insulate itself from Article III scrutiny is a powerful weapon “in the arsenal of . . . arbitrary government.”

The motion should be denied.

FACTS⁵

On June 9, 2005, President Bush assured the public that “Law enforcement officers need a federal judge’s permission to wiretap a foreign terrorist’s phone, a federal judge’s permission to track his calls, or a federal judge’s permission to search his property. Officers must meet strict standards to use any of these tools. And these standards are fully consistent with the Constitution of the U.S.”⁶ Amended Complaint (“Complaint,” or “Compl.”) ¶ 48. As revealed in *The New York Times* in December 2005, however, and as subsequently admitted, *inter alia*, by President Bush, Attorney General Gonzalez, published press reports, whistleblowers, and insiders within the United States government, in the fall of 2001 the National Security Agency (“NSA”)—the intelligence arm of the Department of Defense—launched

⁴*Brinegar v. United States*, 338 U.S. 160, 180 (1949) (Jackson, J., dissenting).

⁵The factual allegations of the Amended Complaint are all accepted as true for purposes of this motion. See *Wilbur v. Locke*, 423 F.3d 1101, 1107 (9th Cir. 2005) (standing); *R.J. Reynolds Tobacco Co. v. Shewry*, 423 F.3d 906, 911 n.2 (9th Cir. 2005) (12(b)(6)).

⁶See <http://www.whitehouse.gov/news/releases/2005/06/20050609-2.html> (President Discusses Patriot Act, dated June 9, 2005).

a secret electronic surveillance program to intercept, search and seize, without prior judicial authorization, the telephone and internet communications of persons inside the United States.

Id. ¶ 50. President Bush secretly approved and reauthorized the program more than 30 times.

Id. ¶¶ 51-52.

The NSA intercepted (and continues to intercept) millions of phone calls and email of ordinary Americans, including plaintiffs, with no connection to Al Qaeda, terrorism, or any foreign government (the “Draagnet” program). The Draagnet program monitors millions of calls and emails made to or from the United States and other countries, and millions of calls and emails entirely within the United States. *Id.* ¶¶ 75-87. The NSA has spied and continues to spy upon these private phone conversations and emails without a warrant. *Id.* ¶¶ 1, 5-8, 83.

Although defendants protest to this Court that the state secrets privilege prevents them from denying the Draagnet program, defendants (as part of this very motion) appear to deny the Draagnet program. *See* Public Declaration of Keith Alexander, May 25, 2007 ¶ 16 (“Plaintiffs’ allegations of a content surveillance draagnet are false.”).

ARGUMENT

I. The Complaint States a Claim for Violation of the Fourth Amendment and FISA

Defendants move to dismiss under Fed. R. Civ. P. 12(b)(1) for lack of subject-matter jurisdiction, and in the alternative, for summary judgment.⁷ Defendants failed to challenge the sufficiency of the Complaint under Rule 12(b)(6), and for good reason. There is no question that, taking the allegations in the Complaint as true, defendants violated the law.

A. The Complaint Alleges Violations of FISA

In 1972, the Supreme Court held that the Fourth Amendment does not permit warrantless surveillance in intelligence investigations of domestic security threats. *See United States v. United States District Court for the Eastern District of Michigan*, 407 U.S. 297 (1972) (“*Keith*”). In 1976, the United States Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, known as the “Church Committee,” found that “warrantless electronic surveillance in the name of national security ha[d] been seriously abused.”⁸ In response to both the *Keith* decision and the Church Committee’s findings, Congress

⁷Defendants’ “summary judgment” motion is perplexing. Defendants do not set forth any set of undisputed facts. Nor do defendants even attempt to argue that their spying program is lawful. Defendants’ “summary judgment” motion is not a summary judgment motion at all, but a jurisdictional state secrets argument in ill-fitting procedural clothes. In any event, the motion, made at the outset of this case, is premature. *See, e.g., TMJ, Inc. v. Nippon Trust Bank*, 2001 WL 925622, at *1 (9th Cir. Aug. 15, 2001); Declaration of Ilann M. Maazel Pursuant to Fed. R. Civ. P. 56(f) in Opposition to Motion to Dismiss Or, in the Alternative, For Summary Judgment, dated July 19, 2007.

⁸S. 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).

passed the Foreign Intelligence Surveillance Act of 1978, an “exclusive charter” intended to “regulate the exercise of [presidential] authority” over intelligence surveillance. S. Rep. No. 95-604(I), at 15-16 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3904, 3916-17. FISA was specifically designed 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, *reprinted in* 1978 U.S.C.C.A.N. at 3910. Congress made clear that it intended to prevent the Executive from engaging in electronic surveillance in the United States without judicial oversight, even during times of war. *See* S. Rep. No. 95-701 (1978), at 47, *reprinted in* 1978 U.S.C.C.A.N. 3973, 4016 (“This bill will establish the exclusive United States law governing electronic surveillance in the United States for foreign intelligence purposes.”).

Congress provided that the procedures set out in FISA and in Title III⁹ “shall be the *exclusive means* by which electronic surveillance . . . and the interception of domestic wire, oral, and electronic communications may be conducted.” 18 U.S.C. § 2511(2)(f) (emphasis added). Rejecting the so-called “inherent authority” Article II argument that the current President seeks to resurrect, Congress expressly rejected language that would have made FISA and Title III the “exclusive *statutory means*” under which electronic surveillance could be conducted, instead adopting language that made those statutes simply the “exclusive means” governing such surveillance. H.R. Conf. Rep. No. 95-1720, at 35 (1978), *reprinted in* 1978 U.S.C.C.A.N. 4048, 4064 (emphasis added); *see* S. Rep. 95-604(I), at 6, *reprinted in* 1978 U.S.C.C.A.N. at 3907 (“The bill recognizes no inherent power of the President in this area.”); S. Rep. 95-604(I), at 16,

⁹Pub. L. No. 90-351, 83 Stat. 311 (1968) (codified as amended at 18 U.S.C. §§ 2510-2522).

reprinted in 1978 U.S.C.C.A.N. at 3917 (“the basis for this legislation is the understanding—concurrent in by the Attorney General—that even if the President has an ‘inherent’ Constitutional power to authorize warrantless surveillance for foreign intelligence purposes, Congress has the power to regulate the exercise of this authority by legislating a reasonable warrant procedure governing foreign intelligence surveillance.”).¹⁰

Congress intended that FISA govern even during emergencies and times of war. In an emergency, FISA permits the Executive to conduct warrantless surveillance for up to 72 hours. *See* 50 U.S.C. § 1805(f). FISA also permits electronic surveillance without a court order for fifteen calendar days after a formal declaration of war. *See* 50 U.S.C. § 1811.

There is no dispute that the Dagnet program involves “electronic surveillance” of Americans. *See* 50 U.S.C. § 1801(f) (defining the term). In order to obtain an order from the FISA Court authorizing electronic surveillance, the government must demonstrate, *inter alia*, probable cause to believe that “the target of the electronic surveillance is a foreign power or an agent of a foreign power” and that “each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a

¹⁰*See* S. Rep. 95-604(I), at 6-7, *reprinted in 1978 U.S.C.C.A.N. at 3908* (FISA “repeal[s] the so-called executive ‘inherent power’ disclaimer clause currently found in Section 2511(3) of Title 18, United States Code. [FISA] provides instead that its statutory procedures (and those found in [Title III]) ‘shall be the exclusive means’ for conducting electronic surveillance, as defined in the legislation, in the United States. The highly controversial disclaimer has often been cited as evidence of a congressional ratification of the President’s inherent constitutional power to engage in electronic surveillance in order to obtain foreign intelligence information essential to the national security. Despite the admonition of the Supreme Court that the language of the disclaimer was ‘neutral’ and did not reflect any such congressional recognition of inherent power, the section has been a major source of controversy. By repealing section 2511(3) and expressly stating that the statutory warrant procedures spelled out in the law *must* be followed in conducting electronic surveillance in the United States, this legislation ends the eight-year debate over the meaning and scope of the inherent power disclaimer clause.”).

foreign power.” 50 U.S.C. § 1805(a)(3); *see* S. Rep. 95-604(I), at 6, *reprinted in* 1978 U.S.C.C.A.N. at 3908 (“[T]he executive cannot engage in electronic surveillance within the United States without a prior judicial warrant.”); S. Rep. 95-604(I), at 18, *reprinted in* 1978 U.S.C.C.A.N. at 3919 (FISA “authorizes electronic surveillance in a limited number of non-criminal situations only under the twin safeguards of an independent review by a neutral judge and his application of a ‘probable cause standard.’”).

Any person who “engages in electronic surveillance under color of law except as authorized by statute” and without “a search warrant or court order” is guilty of a federal crime, “punishable by a fine of not more than \$10,000 or imprisonment for not more than five years, or both.” 50 U.S.C. § 1809. In addition, any “aggrieved person” (defined as any person “whose communications or activities were subject to electronic surveillance,” 50 U.S.C. § 1801(k)), other than a foreign power or an agent of a foreign power, “shall have a cause of action against any person” who violated 50 U.S.C. § 1809. *See* 50 U.S.C. § 1810.

There is no dispute that, taking the allegations in the Complaint as true, defendants violated FISA. As alleged, defendants “engage[d] in electronic surveillance” of plaintiffs without “a search warrant or court order.” 50 U.S.C. §§ 1809(b), 1810.

The Court can also take judicial notice of defendants’ admissions that their program involves electronic surveillance and violates FISA. Defendant Attorney General Gonzales conceded both that “The President has authorized a program to engage in electronic surveillance” (the so-called “Terrorist Surveillance Program” or “TSP”) and that “the Foreign Intelligence Surveillance Act . . . requires a court order before engaging in *this kind of surveillance* that I’ve just discussed and the President announced on Saturday [the TSP], . . .

unless otherwise authorized by statute or by Congress.”¹¹ Defendant Director for National Intelligence Hayden admitted “unequivocally” that the warrantless program was used “in lieu of” FISA.¹² Hayden also stated that the program’s “trigger is quicker and a bit softer than it is for a FISA warrant.”¹³

Taking the allegations of the Complaint as true, as this Court must, the Complaint states a valid claim for violation of FISA.¹⁴

¹¹<http://www.whitehouse.gov/news/releases/2005/12/20051219-1.html> (Press Briefing by Attorney General Gonzalez & General Hayden, Dec. 19, 2005). Defendants of course knew that FISA prohibits the warrantless eavesdropping even of international communications. See S. Rep. No. 95-604(I), at 6, *reprinted in* 1978 U.S.C.C.A.N. at 3907 (“The definition of electronic surveillance has been expanded to include the targeting of United States persons in their international communications. This is specifically aimed at eliminating one of the abuses identified by the Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities and largely implements one of that committee’s recommendations.”).

¹²*Id.* See also http://www.reporter-times.com/?module=displaystory&story_id=30032&format=html (Interview of Homeland Security Secretary Michael Chertoff, Jan. 25, 2006) (“[S]uffice it to say that if you have a large volume of data, a large number of [phone] numbers you’re intercepting, the typical model for any kind of warrant requires you to establish probable cause [that one party is a foreign agent] on an individual number.” But, he continued, FISA warrant applications are “impractical. . . . a voluminous, time-consuming process [I]f you’re culling through literally thousands of phone numbers . . . you could wind up with a huge problem managing the amount of paper you’d have to generate.”).

¹³<http://www.globalsecurity.org/intell/library/news/2006/intell-060123-dni01.htm> (Remarks by General Michael V. Hayden before the National Press Club, Jan. 23, 2006).

¹⁴In *American Civil Liberties Union v. National Security Agency*, 2007 WL 1952370 (6th Cir. July 6, 2007), defendants sought to justify their violation of FISA by claiming that Congress *sub silentio* authorized warrantless surveillance of the American people in the authorization to use force against Al Qaeda (Pub. L. No. 107-40, 115 Stat. 224 (Sept. 18, 2001)), and that the President has “inherent authority” to violate FISA to protect the country. For the reasons thoroughly set forth in the dissent in *ACLU*, (the only opinion in that case to address the merits), both arguments are meritless. *ACLU*, 2007 WL 1952370, at *62-67.

B. The Complaint Alleges Violations of the Fourth Amendment

“The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” U.S. Const. amend. IV. “The security of one’s privacy against arbitrary intrusion by the police—which is at the core of the Fourth Amendment—is basic to a free society.” *Berger v. New York*, 388 U.S. 41, 53 (1967) (citation omitted).

There is little question that, as alleged, the Dagnet violates the Fourth Amendment. A dragnet sweeping hundreds of millions of private phone calls and emails of millions of innocent Americans, without a warrant, probable cause, or even reasonable suspicion, is the very opposite of what the Fourth Amendment requires.

1. The Dagnet is Warrantless

First, the Dagnet program violates the Fourth Amendment because it is warrantless. It has been settled for forty years that the Fourth Amendment requires the government to obtain a warrant before intercepting the content of a telephone call. *See Katz v. United States*, 389 U.S. 347, 352 (1967); *Berger*, 388 U.S. at 51. Wiretapping “[b]y its very nature . . . involves an intrusion on privacy that is broad in scope,” *Berger*, 388 U.S. at 56, and thus bears a dangerous “similarity to the general warrants out of which our Revolution sprang,” *id.* at 64 (Douglas, J., concurring). Warrants are *particularly* vital in the wiretapping context. For “[f]ew threats to liberty exist which are greater than that posed by the use of eavesdropping

devices.” *Berger*, 388 U.S. at 63. A wiretap “constitutes a dragnet, sweeping in all conversations within its scope—without regard to the participants or the nature of the conversations. It intrudes upon the privacy of those not even suspected of crime and intercepts the most intimate of conversations.” *Id.* at 65 (Douglas, J., concurring).

Any search conducted without a warrant is presumptively unreasonable. “Over and again this Court has emphasized that the mandate of the Fourth Amendment requires adherence to judicial processes, and that searches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions.” *Katz*, 389 U.S. at 357 (citation and footnotes omitted); *see also United States v. Karo*, 468 U.S. 705, 717 (1984); *Payton v. New York*, 445 U.S. 573, 586 (1980); *Chimel v. California*, 395 U.S. 752, 762-63 (1969). The warrant requirement is no mere “formalit[y]. The presence of a search warrant serves a high function. Absent some grave emergency, the Fourth Amendment has interposed a magistrate between the citizen and the police.” *McDonald v. United States*, 335 U.S. 451, 455 (1948). “The right of privacy was deemed too precious to entrust to the discretion of those whose job is the detection of crime and the arrest of criminals.” *Id.* at 455-56.

The Supreme Court has never recognized an exception to the warrant requirement for intelligence surveillance inside the United States. To the contrary, in the *Keith* case, the Supreme Court rejected such an exception, holding that the Fourth Amendment’s promise of privacy “cannot properly be guaranteed if security surveillance may be conducted solely within the discretion of the Executive Branch.” 407 U.S. at 316-17. In the intelligence context, as elsewhere, “[t]he warrant clause of the Fourth Amendment is not dead language. Rather, it has

been a valued part of our constitutional law for decades It is not an inconvenience to be somehow ‘weighed’” against the government’s interests. *Id.* at 315 (citation omitted). In the intelligence context, as elsewhere, “unreviewed executive discretion may yield to pressures to obtain incriminating evidence and overlook potential invasions of privacy and protected speech.” *Id.* at 317. In the intelligence context, as elsewhere, “[p]rior review by a neutral and detached magistrate is the time-tested means of effectuating Fourth Amendment rights.” *Id.* at 318.¹⁵

In *Keith*, the Supreme Court rejected every argument the President makes today for a warrantless eavesdropping intelligence program. “It is urged that the requirement of prior judicial review would obstruct the President in the discharge of his constitutional duty to protect domestic security.” The Court rejected the argument. *Id.* at 318. “We are told further that these surveillances are directed primarily to the collecting and maintaining of intelligence with respect to subversive forces, and are not an attempt to gather evidence for specific criminal prosecutions.” The Court rejected this “prevention, not prosecution” argument. *Id.* at 318-19. “The Government further insists that courts . . . have neither the knowledge nor the techniques necessary to determine” whether the “surveillance was necessary to protect national security,” issues that “involve a large number of complex and subtle factors beyond the competence of courts to evaluate.” The Court rejected this argument too, even before almost three decades of experience with FISA demonstrated its invalidity. *Id.* at 319. As its trump card, the same card the Executive would use today, “the Government believes that disclosure to a magistrate of all or

¹⁵Congress agrees with the Supreme Court. FISA “embodies a legislative judgment that court orders and other procedural safeguards are necessary to insure that electronic surveillance by the U.S. Government within this country conforms to the fundamental principles of the Fourth Amendment.” S. Rep. No. 95-701, at 13, *reprinted in* 1978 U.S.C.C.A.N. at 3982.

even a significant portion of the information involved” in the surveillance would endanger “the national security and . . . the lives of informants and agents Secrecy is the essential ingredient in intelligence gathering.” The Supreme Court rejected that argument too. *Id.*

Instead, the Court held that “Official surveillance, whether its purpose be criminal investigation or ongoing intelligence gathering, risks infringement of constitutionally protected privacy of speech. Security surveillances are especially sensitive because of the inherent vagueness of the domestic security concept, the necessarily broad and continuing nature of intelligence gathering, and the temptation to utilize such surveillance to oversee political dissent.” *Id.* at 320. Although the warrant procedure imposes an “added burden” upon the Executive, “this inconvenience is justified in a free society to protect constitutional values.” *Id.* at 321. “[B]y no means of least importance,” the warrant will “reassur[e] . . . the public generally that *indiscriminate wiretapping and bugging of law-abiding citizens cannot occur*,” *id.* (emphasis added), which is precisely what the Complaint alleges happened when this President decided to bypass the warrant requirement.

Keith concerned surveillance relating to domestic security threats rather than foreign security threats but the *Keith* Court’s reasoning applies with equal force here. *See Zweibon v. Mitchell*, 516 F.2d 594, 614 (D.C. Cir. 1975) (plurality opinion) (requiring a warrant even where surveillance “is installed under presidential directive in the name of foreign intelligence gathering for protection of the national security”); *id.* at 651 (“absent exigent circumstances, no wiretapping in the area of foreign affairs should be exempt from prior judicial scrutiny, irrespective of the justification of the surveillance or the importance of the information sought”); *id.* at 689 (Wilkey, J., concurring) (warrantless surveillance violates Fourth

Amendment notwithstanding President's "foreign affairs" power).¹⁶ A neutral intermediary between Americans and executive officers is no less necessary because the threat comes from foreign agents rather than domestic ones. In the absence of judicial oversight, no one can even be sure that surveillance targets *are* foreign agents. In this case, for example, the Complaint alleges that defendants are surveilling millions of Americans who plainly have nothing to do with foreign agents or governments. As a result, the so-called "foreign intelligence surveillance" at issue presents exactly the same dangers as the "domestic intelligence surveillance" in *Keith*.

Nor are any of the rationales the government presented in *Keith* for warrantless domestic intelligence surveillance any more convincing in the foreign intelligence context. *See Zweibon*, 516 F.2d at 641-651 (summarizing and methodically rejecting every government rationale for warrantless foreign intelligence surveillance in the United States). The judiciary is, if anything, more qualified to deal with national security issues than when *Keith* was decided, because it now has almost thirty years of experience with FISA. FISA also forecloses any argument that the warrant requirement can be dispensed with simply because the Executive claims its actions are directed at foreign agents. As the Senate Intelligence Committee explained, FISA "embodies a legislative judgment that court orders and other procedural safeguards are necessary to insure that electronic surveillance by the U.S. government within this country conforms to the fundamental principles of the Fourth Amendment." S. Rep. No. 95-701, at 13, *reprinted in* 1978 U.S.C.C.A.N. at 3982.

¹⁶Thus, a majority of the D.C. Circuit agreed that warrants are required for foreign electronic intelligence surveillance, at least vis-a-vis domestic organizations that are not agents for or acting in collaboration with a foreign power. *Id.* at 614, 689.

“[G]iven the way in which almost any activity can be said to relate, at least remotely, to foreign affairs or foreign policy making, the potential scope of [a foreign intelligence] exception to the warrant requirement is boundless, and thus a substantial danger to the values the Fourth Amendment was fashioned to protect.” *Zweibon*, 516 F.2d at 654. This case, involving a massive sweep of domestic communications of innocent Americans in the name of fighting a foreign enemy, could not make that point more clearly. Because the Dragnet is warrantless, it violates the Fourth Amendment.

2. The Dragnet is General and Indiscriminate, Not Specific and Particularized

Second, the Dragnet program—which spies upon millions of Americans—violates the Fourth Amendment’s proscription against general searches. The use of “general warrants” was “a motivating factor behind the Declaration of Independence The Fourth Amendment’s requirement that a warrant ‘particularly describ(e) the place to be searched, and the persons or things to be seized,’ repudiated these general warrants and makes general searches impossible.” *Berger*, 388 U.S. at 58 (citing the Fourth Amendment); *see also Chimel*, 395 U.S. at 761 (“The [Fourth] Amendment was in large part a reaction to the general warrants and warrantless searches that had so alienated the colonists and had helped speed the movement for independence.”). The Dragnet is even worse than a general warrant, because it is a general search without a warrant. The Dragnet does not target any “particular[] . . . place to be searched” or “persons or things to be seized.” U.S. Const. amend. IV. Rather, it indiscriminately targets every call and every email of every person. No such general search has ever been permitted in any Fourth Amendment case. *See, e.g., Berger*, 388 U.S. at 57 (“The need for particularity and evidence of reliability in the

showing required when judicial authorization of a search is sought is especially great in the case of eavesdropping.”); *id.* at 58 (The “indiscriminate use of electronic devices” is to be “condemned”) (citation omitted); *id.* (“[G]eneral searches by electronic devices” are of “truly offensive character” and violate the Fourth Amendment); *id.* at 59 (Even a “statute’s failure to describe with particularity the conversations sought gives the officer a roving commission to ‘seize’ any and all conversations. As with general warrants this leaves too much to the discretion of the officer executing the order.”).

3. The Dragnet is Not Reasonable Or Based Upon Probable Cause

Third, the Dragnet violates the Fourth Amendment because the indiscriminate eavesdropping of millions of Americans is “unreasonable” and not based on “probable cause.” *Id.* The Dragnet sweeps millions of Americans, even though there is no probable cause to believe either that they committed a crime, *Berger*, 388 U.S. at 59, or that they are an “agent of a foreign power.” 50 U.S.C. § 1805(a)(3). The Supreme Court held forty years ago that wiretapping without probable case violates the Fourth Amendment. *See Berger*, 388 U.S. at 64 (Douglas, J., concurring) (*Berger* “allows a discreet surveillance *only* on a showing of ‘probable cause.’”) (emphasis added); *id.* at 59 (majority opinion) (“The purpose of the probable cause requirement of the Fourth Amendment” is “to keep the state out of constitutionally protected areas until it has reason to believe that a specific crime has been or is being committed.”).

“[I]t is not asking too much that [defendants] be required to comply with the basic command of the Fourth Amendment before the innermost secrets of one’s home or office are invaded.” *Berger*, 388 U.S. at 63. Defendants do not challenge the sufficiency of plaintiffs’

Fourth Amendment claim because they cannot. As alleged, defendants violated the Fourth Amendment.

II. The Executive's Radical Extension of the State Secrets Privilege Cannot Bar This Suit

Rather than attempt to defend the indefensible, defendants seek to avoid the merits by transforming a narrow, evidentiary privilege into a sweeping immunity for violations of criminal law and the Constitution. The effort should be rejected.

A. FISA Itself Precludes Application of the State Secrets Privilege In This Case

The state secrets privilege is no more than “an evidentiary privilege rooted in federal common law.” *Kasza v. Browner*, 133 F.3d 1159, 1167 (9th Cir. 1998); *In re United States*, 872 F.2d 472, 474 (D.C. Cir. 1989) (“The state secrets privilege is a common law evidentiary rule.”). Where a statute “speaks directly to [a] question otherwise answered by federal common law,” the statute preempts common law. *Kasza*, 133 F.3d at 1167 (citations omitted); *see Dickerson v. United States*, 530 U.S. 428, 437 (2000) (“Congress retains the ultimate authority to modify or set aside any judicially created rules of evidence and procedure that are not required by the Constitution.”) (citation omitted).

As multiple courts have recognized, Congress may preempt the state secrets privilege, as well as the more narrow espionage agreement privilege (*see infra* § II(D)). *See Halpern v. United States*, 258 F.2d 36, 43 (2nd Cir. 1958) (“Unless Congress has created rights which are completely illusory, existing only at the mercy of government officials, the act must be viewed as waiving the [state secrets] privilege.”); *Kasza*, 133 F.3d at 1167; *Tenet v. Doe*, 544

U.S. 1, 11 (2005) (where “the national interest would be well served . . . Congress can modify the federal common-law rule announced in *Totten*”) (Stevens, J., concurring).¹⁷

Here, there is little question that Congress has, through FISA, directly addressed the procedures for handling confidential information. FISA, not the state secrets privilege, controls in this case, and FISA plainly does not authorize dismissal on state secrets grounds.

1. The FISA Cause of Action is Inconsistent With the State Secrets Privilege

FISA Section 1810, by providing a private cause of action for FISA violations despite the otherwise secret nature of FISA proceedings, plainly displaces any common law rule of outright dismissal. If Section 1810 did not preclude outright dismissal, then Congress’

¹⁷To the extent the state secrets privilege is related to the President’s Article II powers, as a couple of lower court cases have suggested, the Executive nevertheless may not ignore a Congressional statute. *See, e.g., United States v. Nixon*, 418 U.S. 683, 715 (1974) (the President is not “above the law”); *Hamdi v. Rumsfeld*, 542 U.S. 507, 536 (2004) (plurality opinion) (“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.”); *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 the Congress has, in proper exercise of its own war powers, placed on his powers.”); *id.* at 2799 (Kennedy, J., concurring) (“Congress, in the proper exercise of its powers as an independent branch of government . . . set limits on the President’s authority.”). “When the President takes measures incompatible with the expressed or implied will of Congress, his power is at its lowest ebb.” *Youngstown*, 343 U.S. at 637 (Jackson, J., concurring). Here Congress has plainly spoken as to how confidential information should be treated in a FISA case, exercising its authority to override the privilege. *See, e.g., Halpern*, 258 F.2d at 43; *Kasza*, 133 F.3d at 1167; *Tenet*, 544 U.S. at 11. Like the statutes at issue in *Youngstown* and *Hamdan*, FISA was the result of “a deliberative and reflective process engaging both of the political branches.” *Hamdan*, 126 S.Ct. at 2799; *see also Youngstown*, 343 U.S. at 660 (Burton, J., concurring) (“The controlling fact here is that Congress, within its constitutionally delegated power, has prescribed for the President specific procedures . . . for his use in meeting the present type of emergency.”). The President, therefore, cannot disregard the limitations that Congress, through FISA, has properly placed on executive power.

creation of a private FISA action would be meaningless, for the President would be able to evade any FISA claim merely by invoking the state secrets privilege.

The situation is analogous to *Halpern v. U.S.*, 258 F.2d 36 (2nd Cir. 1958), a lawsuit arising under the Invention Secrecy Act, 35 U.S.C. § 181 *et seq.*, which allowed the patent office to withhold a patent grant for inventions implicating national security, but also allowed inventors to sue for compensation if a patent was denied. When the plaintiff was denied a patent and sued for compensation, the government invoked the state secrets privilege. The Second Circuit rejected the assertion of the privilege because “the trial of cases involving patent applications placed under a secrecy order will always involve matters within the scope of this privilege,” and “[u]nless Congress has created rights which are completely illusory, existing only at the mercy of government officials, the Act must be viewed as waiving the privilege.” *Id.* at 43. *Halpern* specifically distinguished *United States v. Reynolds*, 345 U.S. 1 (1953), which did not “involv[e] a specific enabling statute contemplating the trial of actions that by their very nature concern security information.” *Id.* at 44.

Similarly, a private FISA action (which by definition concerns “Foreign Intelligence Surveillance”) involves matters that “by their very nature concern security information.” *Id.* Unless Section 1810 creates “rights which are completely illusory, existing only at the mercy of government officials,” *id.*, FISA must be viewed as supplanting the state secrets privilege, vesting courts with the power to ensure national security with “appropriate security procedures and protective orders.” 50 U.S.C. § 1806(f).

2. In Addition to Creating a Cause of Action, Congress Set Forth Specific Procedures to Govern Confidential Information Relating to Electronic Surveillance

Congress did not merely create a private cause of action under FISA, it set forth a detailed procedure for courts to follow whenever the Government invokes the state secrets privilege in cases involving electronic surveillance. *See* 50 U.S.C. § 1806(f).

The five-step protocol outlined in Section 1806(f) 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. Following such request, “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 relating to 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. Where disclosure to the plaintiff is necessary, the court discloses the materials subject to “appropriate security procedures and protective orders.” *Id.*

This procedure applies, without qualification and “notwithstanding any other law,” to discovery of any materials relating to “electronic surveillance,” which includes any “acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication . . . without the consent of any party thereto.” *Id.*; 50 U.S.C. § 1801(f)(2); *see*

also S. Rep. No. 95-604(I), at 57, *reprinted in* 1978 U.S.C.C.A.N. at 3958 (procedures “apply whatever the underlying rule or statute referred to in [a party’s] motion.”).

The detailed procedures set forth in Section 1806(f) apply whether or not the Executive has acknowledged the challenged surveillance. *See Al-Haramain Islamic Found. v. Bush*, 451 F.Supp.2d 1215, 1231 (D.Or. 2006) (“To accept the government’s argument that Section 1806(f) is only applicable when the government intends to use information against a party would nullify FISA’s private remedy and would be contrary to the plain language of Section 1806(f).”). The procedure set forth in Section 1806(f) is not merely applicable, but the exclusive means by which the Executive can assert the state secrets privilege over information related to electronic surveillance. When the legality of the surveillance is at issue, “it is this procedure ‘notwithstanding any other law’ that must be used to resolve the question.” S. Rep. No. 95-604(I), at 57, *reprinted in* 1978 U.S.C.C.A.N. at 3958.

3. FISA Also Contemplated Discovery From Telecommunications Carriers

The civil cause of action against private parties for violations of FISA, *see* 18 U.S.C. §§ 2520, 2511(2)(a)(ii), further confirms that Congress intended to preempt the state secrets privilege in electronic surveillance cases. FISA amended 18 U.S.C. § 2511(2)(a)(ii) (1970) to specify that a “communications common carrier” must receive either a court order or a certification that the prospective electronic surveillance is legal before it may help the government monitor customer communications. FISA § 201(a). As a result, if a telephone company assists the government in conducting surveillance without a Section 2511 court order or certification, it is liable for damages under 18 U.S.C. § 2520.

Congress was clearly aware that sensitive information would be at issue in litigation over the legality of cooperation between carriers and the government under Section 2511(2)(a)(ii). To address the possibility, Congress forbade carriers from disclosing information relating to these surveillance efforts *except as "required by legal process."* FISA § 201(a) (amending 18 U.S.C. § 2511(2)(a)(ii)) (emphasis added). In the event legal process does require the carrier to disclose confidential information, the carrier must first give notice to the Attorney General or another authority. *Id.*

Read in conjunction with 50 U.S.C. § 1806(f), the notice provision in Section 2511(2)(a)(ii) is further evidence that Congress fully considered and addressed the need for both secrecy and discovery, even in litigation involving surveillance efforts aided by common carriers.

4. FISA Precludes Dismissal

FISA nowhere permits dismissal of an action simply because it may involve confidential information. To the contrary, FISA sets forth an explicit procedure for handling confidential information as the case goes forward. *See* 50 § 1806(f). The five-step protocol established by Congress provides plaintiffs an opportunity to pursue their claim while guarding against unnecessary disclosures of secret information. The Court must decide “whether the surveillance of the aggrieved person was lawfully authorized and conducted” and, if necessary, disclose the evidence to the aggrieved party under appropriate circumstances. *Id.*; *ACLU Found. of Southern Cal. v. Barr*, 952 F.2d 457, 465, 470 (D.C. Cir. 1991) (Section 1806(f) procedures “[a]re not to be bypassed by the inventive litigant using a new statute, rule or judicial

construction.”) (citation omitted). But FISA contains no reference to dismissal, on the pleadings or otherwise. Section 1806(f) is an unambiguous rejection of such premature termination of litigation in the electronic surveillance context.

Halpern governs this case, not *Reynolds*. Where, as here, Congress has enacted legislation that evinces its “intent to replace the government’s evidentiary privilege to withhold sensitive information” with a different protocol, the common law privilege is preempted. *Kasza*, 133 F.3d at 1168; *Halpern*, 258 F.2d at 43; *Tenet*, 544 U.S. at 11. Congress may not only draw the line between personal liberty and national security, as it has in enacting FISA and the other statutes at issue, it may lay down a specific procedure for courts to employ to determine whether that line has been crossed. That is what FISA has done here. Defendants’ motion should be denied.

B. Origins of the State Secrets Privilege and Constitutional Principles At Stake

Defendants’ argument is breathtaking. If the Executive successfully uses the state secrets privilege to dismiss this case at the pleading stage, there will be virtually no check left upon the ability of an overly-aggressive executive to violate the rights of ordinary Americans. With a single declaration, the Executive can wipe out statutory mandates, immunize himself from Article III scrutiny, and arrogate to himself the power to engage in unconstitutional and even criminal conduct, for however long, affecting millions. This startling departure from over two hundred years of American jurisprudence must be rejected.

Part 2 to Plaintiffs' Memorandum of Law
In Opposition to Motion to Dismiss or For Summary Judgment
by the United States and the Official Capacity Defendants

(In *Shubert v. Bush*, 07-693)

1. Principles of Separation of Powers

“It is emphatically the province and duty of the judicial department to say what the law is.” *Marbury v. Madison*, 5 U.S. 137, 177 (1803). This duty is especially great where constitutional rights are at stake. “[A]lthough the attempt to claim Executive prerogatives or infringe liberty in the name of security and order may be motivated by the highest of ideals, the judiciary must remain vigilantly prepared to fulfill its own responsibility to channel Executive action within constitutional bounds.” *Zweibon*, 516 F.2d at 604 (plurality opinion). It is particularly “the duty of the courts to be watchful for the constitutional rights of the citizen, and against any stealthy encroachments thereon.” *Reid v. Covert*, 354 U.S. 1, 40 (1957) (citation omitted). Here the Executive seeks through the back door of a narrow, common law evidentiary privilege to undermine at least four major constitutional principles: the right of plaintiffs to be free from unreasonable searches and seizures, *see* U.S. Const. amend. IV; the right of plaintiffs to a judicial forum to assert their constitutional rights, *see Webster v. Doe*, 486 U.S. 592, 603 (1988); the constitutional right and duty of Article III courts to “say what the law is,” *Marbury*, 5 U.S. at 177; and the constitutional limitations upon the Executive to exert power unauthorized by Congress within the domestic sphere, *see Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 587 (1952).

“Ours is a government of divided authority on the assumption that in division there is not only strength but freedom from tyranny.” *Reid*, 354 U.S. at 40; *The Federalist No. 47* (James Madison) (“The accumulation of powers, legislative, executive, and judiciary in the same hands . . . may justly be pronounced the very definition of tyranny”); *Hamdan*, 126 S.Ct. at 2800 (Kennedy, J., concurring) (“Concentration of power puts personal liberty in peril of

arbitrary action by officials, an incursion the Constitution's three-part system is designed to avoid."). These fundamental separation of powers principles and the obligations of Article III courts are not altered in wartime. In *Hamdi v. Rumsfeld*, 542 U.S. 507 (2004), which reversed on due process grounds the dismissal of a citizen "enemy combatant's" petition for habeas corpus, the Supreme Court held that "we have long since made clear that a state of war is not a blank check for the President when it comes to the rights of the Nation's citizens." *Id.* at 536 (plurality opinion); see *Ex Parte Milligan*, 71 U.S. 2, 120 (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. No doctrine, involving more pernicious consequences, was ever invented by the wit of man than that any of its provisions can be suspended during any of the great exigencies of government."); *Youngstown Sheet*, 343 U.S. at 650 (Jackson, J., concurring) ("Aside from suspension of the privilege of the writ of habeas corpus in time of rebellion or invasion, when the public safety may require it, [the founders] made no express provision for exercise of extraordinary authority because of a crisis. I do not think we rightfully may so amend their work."). "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." *Hamdi*, 542 U.S. at 536 (plurality opinion).

Another core constitutional principle—relevant to the extent defendants argue that the state secrets privilege is rooted in Article II—is the President's traditional *inability* to assert Commander-in-Chief and "foreign affairs" powers within the domestic sphere. In the great *Steel Seizure* case, striking down President Truman's executive order seizing steel production facilities

in order to avert a strike during the Korean War, the Supreme Court held that the President's power does not extend to regulating private domestic activities, however connected to the actual conduct of war: "The order cannot properly be sustained as an exercise of the President's military power as Commander in Chief of the Armed Forces Even though 'theater of war' be an expanding concept, we cannot with faithfulness to our constitutional system hold that the Commander in Chief of the Armed Forces has the ultimate power as such to take possession of private property in order to keep labor disputes from stopping production. This is a job for the Nation's lawmakers, not for its military authorities." *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 587 (1952).

The Complaint, of course, alleges that the President has expanded "foreign" warrantless intelligence surveillance into the homes of millions of ordinary Americans within the United States. The President has admitted to authorizing a warrantless spying program upon thousands of persons in the United States, where at least one party to the call is within the United States.¹⁸ The Complaint alleges that defendants' spying program is even broader, involving a warrantless surveillance dragnet of millions of calls and emails by millions of people within the United States, both where the calls/emails are entirely within the United States, and where at least one end of the calls/emails are within the United States. *See* Compl. ¶¶ 1-3, 53-90. In short the Complaint alleges a domestic spying program, in the United States, affecting millions of American citizens, most of whom have never even traveled abroad on holiday, much less to affiliate with the Al Qaeda terrorist network. This case falls within the heartland of *Youngstown*,

¹⁸See <http://www.whitehouse.gov/news/releases/2005/12/20051219-1.html>

another factor the Court must consider when evaluating defendants' sweeping claims of privilege.

Another core separation of powers principle applicable here is "the deeply rooted and ancient opposition in this country to the extension of military control over civilians." *Reid*, 354 U.S. at 33; *see id.* at 23-24 ("The Founders envisioned the army as a necessary institution, but one dangerous to liberty if not confined within its essential bounds."); *Laird v. Tatum*, 408 U.S. 1, 15 (1972) (recognizing "a traditional and strong resistance of Americans to *any military intrusion into civilian affairs*" that "has deep roots in our history") (emphasis added); *Youngstown Sheet*, 343 U.S. at 632 (Douglas, J., concurring) ("[O]ur history and tradition rebel at the thought that the grant of military power carries with it authority over civilian affairs."); *Toth v. Quarles*, 350 U.S. 11, 13 (1955) ("[A]ssertion of military authority over civilians cannot rest on the President's power as commander-in-chief, or on any theory of martial law."); *Al-Marri v. Wright*, 2007 WL 1663712, at *27 (4th Cir. June 11, 2007) ("[A]bsent suspension of the writ of habeas corpus or declaration of martial law, the Constitution simply does not provide the President the power to exercise military authority over civilians within the United States."). As the Supreme Court wrote in 1957, "[t]he country ha[d] remained true to that faith," a faith "firmly embodied in the Constitution," for "almost one hundred seventy years." *Reid*, 354 U.S. at 40. "Another half century has passed but the necessity of 'remain [ing] true to that faith' remains as important today as it was at our founding." *Al-Marri*, 2007 WL 1663712, at *28.

This core constitutional principle is very much at stake here, where the President seeks to justify a spying program upon the American people by the intelligence arm of the Department of Defense, based upon a war against a foreign terrorist organization. "[N]o doctrine

that the Court could promulgate would seem . . . more sinister and alarming than that a President whose conduct of foreign affairs is so largely uncontrolled, and often even is unknown, can vastly enlarge his mastery over the internal affairs of the country by his own commitment of the Nation's armed forces to some foreign venture." *Youngstown Sheet*, 343 U.S. at 642 (Jackson, J., concurring).

2. The State Secrets Privilege

With this backdrop, we turn to the doctrine of the state secrets privilege. The origins of the privilege in this country date to the Aaron Burr trial, in which Burr moved for a *subpoena duces tecum* ordering President Jefferson to produce a letter by General James Wilkinson. The government argued "that the letter contains material which ought not to be disclosed." Riding circuit, Chief Justice Marshall held that if the letter "contain[s] any matter which it would be imprudent to disclose, which it is not the wish of the executive to disclose, such matter, *if it be not immediately and essentially applicable to the point*, will, of course, be suppressed." *United States v. Burr*, 25 F.Cas. 30, 37 (C.C.D.Va. 1807) (emphasis added). Of course, if the material were "immediately and essentially applicable to the point," it would not be suppressed, notwithstanding the "impruden[ce]" of disclosure. *Id.*

After *Burr*, two doctrines developed: a narrow doctrine covering espionage agreements, and a somewhat broader state secrets doctrine. The first espionage case was *Totten v. United States*, 92 U.S. 105 (1875). There, the administrator of a former spy's estate sued the government based on a contract the spy allegedly made with President Lincoln to recover compensation for espionage services rendered during the Civil War. *Id.* at 105-06. The *Totten*

Court barred the action because “[t]he service stipulated by the contract was a secret service; the information sought was to be obtained clandestinely, and was to be communicated privately; the employment and the service were to be equally concealed. Both employer and agent must have understood that the lips of the other were to be for ever sealed respecting the relation of either to the matter. This condition of the engagement was implied from the nature of the employment.” *Id.* at 106. In short, the plaintiff’s decision to become a spy operated as a waiver of his ability to enforce the espionage agreement. In *Tenet v. Doe*, 544 U.S. 1 (2005), the Court essentially reaffirmed *Totten*, holding that two alleged Cold War spies could not sue the CIA to enforce an espionage agreement.

Like the limited espionage doctrine, the state secrets privilege first grew out of cases involving persons who worked with or for the military. The first modern state secrets case, *United States v. Reynolds*, 345 U.S. 1 (1953), arose out of the death of individuals who volunteered to observe a secret test run of a B-29 aircraft carrying sensitive military equipment. *Id.* at 3. The decedents chose to volunteer for a sensitive military mission, and as in *Totten*, plainly must have known that the mission was to remain a secret. After the flight crashed, killing three civilian observers, their widows sued the government under the Federal Tort Claims Act and sought discovery of the Air Force’s official accident investigation report. *Id.* at 2-3. The Secretary of the Air Force filed a formal “Claim of Privilege” and refused to produce the accident report. *Id.* at 4-5. Defendants, however, did volunteer to “produce the three surviving crew members, without cost, for examination by the plaintiffs” in a sworn deposition, *id.* at 5, an offer plaintiffs rejected, *id.* at 11. There was also little reason to believe that the secret information

(concerning the sensitive “electronic equipment”) had “any causal connection with the accident,” and therefore there was little necessity for the accident report. *Id.* at 11.

Reynolds first defined the state secrets privilege. It applies *only* where a court is satisfied “from all the circumstances of the case,” that (1) “there is a reasonable danger that compulsion of the evidence” will (2) “expose *military matters*” which (3) “in the interest of national security, should not be divulged.” 345 U.S. at 10 (emphasis added). *Reynolds* did not extend the privilege to *any* matter that could impair national security, only “military matters.” *Id.* “When this is the case,” *i.e.*, when this three-part test is met, “the occasion for the privilege is appropriate.” *Id.*¹⁹

The *Reynolds* Court noted that “[j]udicial control over the evidence in a case cannot be abdicated to the caprice of executive officers.” *Id.* at 9-10. Yet, at least where “military matters” which “in the interest of national security, should not be divulged” are concerned, the Court did not require that the government “automatically” provide “complete disclosure” of the secret information before the claim of privilege would be accepted. *Id.* The Court further held that “[i]n each case, the showing of necessity which is made will determine how far the court should probe in satisfying itself that the occasion for invoking the privilege is appropriate. Where there is a strong showing of necessity, the claim of privilege should not be lightly accepted.” *Id.* at 11. The Court also held that “even the most compelling necessity cannot overcome the claim of privilege if the court is ultimately satisfied that military secrets are at

¹⁹The *Reynolds* Court also imposed certain minimal procedural requirements: the state secrets privilege “belongs to the Government and must be asserted by it There must be a formal claim of privilege, lodged by the head of the department which has control over the matter, after actual personal consideration by that officer.” *Id.* at 7-8

stake.” *Id.* The *Reynolds* Court, of course, had no occasion to consider whether this would be the case outside the context of *Totten* and *Reynolds*, where plaintiffs themselves contracted with or worked with the military.

The *Reynolds* holding was perfectly sensible. The case plainly dealt with a “military matter,” *i.e.*, a military mission involving persons flying on a military aircraft. The Court’s decision was also animated by another critical factor: plaintiffs had little necessity for the withheld information. “[W]here necessity is dubious, a formal claim of privilege, made under the circumstances of this case, will have to prevail.” *Id.* at 11. In *Reynolds*, necessity was “dubious,” because it was “greatly minimized by an available alternative [sworn depositions of the surviving crew], which might have given respondents the evidence to make out their case without forcing a showdown on the claim of privilege. By their failure to pursue that alternative, respondents have posed the privilege question for decision with the formal claim of privilege set against a dubious showing of necessity.” *Id.*

Another critical factor in *Reynolds* was the lack of any reason “to suggest that the electronic equipment . . . had any causal connection with the accident. Therefore, it should be possible for respondents to adduce the essential facts as to causation without resort to material touching upon military secrets.” As the Court held, “[r]espondents were given a reasonable opportunity to do just that, when petitioner formally offered to make the surviving crew members available for examination. We think that offer should have been accepted.” *Id.*²⁰

²⁰As noted in § II(A), *supra*, *Reynolds* also did not involve a statute “contemplating the trial of actions that by their very nature concern security information.” *Halpern*, 258 F.2d at 44. Where, as here, such a statute applies, the state secrets privilege does not apply. *Id.* (expressly distinguishing *Reynolds*).

The *Reynolds* holding must therefore be understood within the context of (1) a plainly military operation, involving (2) decedents who chose to join the military mission, and (3) plaintiffs who had at best a “dubious” need to learn about state secrets that (4) were not even causally related to the claim, and who (5) refused alternative methods of discovery (such as depositions) to prove their case. *Reynolds* also did not have occasion to consider the privilege in the context of executive encroachment into the domestic sphere, *cf. Youngstown Sheet*, nor in the context of the “military[’s] intrusion into civilian affairs,” *Laird*, 408 U.S. at 15. Nor did *Reynolds* consider the privilege in the context of a plaintiff asserting constitutional claims. *Cf. Webster v. Doe*, 486 U.S. 592 (1988).

Like this case, however, *Webster* did involve constitutional claims. There, an employee fired by the Central Intelligence Agency (apparently because of his sexual orientation) brought claims against the agency under, *inter alia*, the First, Fourth, Fifth and Ninth Amendments of the Constitution. The Supreme Court held that Section 102(C) of the National Security Act of 1947 could not exclude judicial review of the constitutional claims. *Id.* at 603. In reaching that conclusion, the Court noted the “serious constitutional question that would arise if a federal statute were construed to deny any judicial forum for a colorable constitutional claim.” *Id.* (citation omitted). Although the Director of the Central Intelligence Agency “complain[ed] that judicial review even of constitutional claims will entail extensive rummaging around in the Agency’s affairs to the detriment of national security,” *id.* at 604, the Court permitted the case to go forward. Citing *Reynolds*, the Court gave the district court “latitude to control any discovery process which may be instituted so as to balance respondent’s need for access to proof which would support a colorable constitutional claim against the extraordinary

needs of the CIA for confidentiality and the protection of its methods, sources, and mission.” *Id.* Thus, thirty-five years after *Reynolds*, the Supreme Court authorized courts—at least in cases asserting constitutional claims—to “balance[]” plaintiff’s “need for access to proof” as against the “extraordinary” national security needs of the government. *Id.*

(i) The Ninth Circuit and the State Secrets Privilege

Kasza v. Browner, 133 F.3d 1159 (9th Cir. 1998), like *Reynolds* a tort case involving no constitutional claims, is the leading Ninth Circuit case on the state secrets privilege. Like *Totten*, *Tenet*, and *Reynolds*, and unlike this case, *Kasza* involved plaintiffs working for or with the United States military. Plaintiffs were former workers at a classified Air Force facility who brought environmental tort claims arising from conduct on the military facility itself. *Id.* at 1162. Like *Reynolds*, *Kasza* did not involve any encroachment of the executive into the domestic sphere, *cf. Youngstown Sheet*, nor any “military intrusion into civilian affairs,” *Laird*, 408 U.S. at 15, nor any constitutional claims, *cf. Webster*, much less claims affecting fundamental checks and balances, separation of powers, and the compelling Fourth Amendment claims set forth here. *Kasza* was a tort case on behalf of workers at a military base, concerning matters on the base.

Even though the two related cases in *Kasza* concerned conduct on a military base, and even though neither case raised any constitutional claim, neither case was dismissed at the outset of the litigation. Rather, in the first case (Frost) “discovery got underway,” *Kasza*, 133 F.3d at 1163, then the Air Force refused on state secrets grounds to provide most documents plaintiffs requested, concerning operations on the base. At the conclusion of discovery, the Court granted the Air Force summary judgment. *Id.* In the related *Kasza* action, the government produced declarations refuting plaintiff’s claims on the merits, as well as inventory and

inspection reports to the court *in camera*. *Id.* at 1164. Based upon those reports, the district court ruled that, as to various injunctive claims, defendants were already providing relief and the claims were moot. The court also denied defendants' summary judgment motion on other claims, a ruling later mooted by subsequent events. *Id.*

The *Kasza* court, again carefully limiting the state secrets privilege to "military matters," held that, for the government to successfully withhold evidence claiming state secrets, the government must satisfy the court "under the particular circumstances of the case" that "there is a reasonable danger that compulsion of the evidence will expose military matters which, in the interest of national security, should not be divulged." *Kasza*, 133 F.3d at 1166. The court concluded that release of information about activity on the Air Force base would reasonably endanger national security interests, *id.* at 1170, and affirmed the grant of summary judgment.

(ii) Other Circuits and the State Secrets Privilege

Only a handful of state secrets cases in other circuits have dealt with issues similar to those in this case, and those cases (1) predated *Webster*, and (2) did not involve a statute such as FISA, *cf. Halpern*, 258 F.2d at 43-44. In *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*"), plaintiffs sued the government to enjoin alleged wiretapping by the government. In neither case did the court simply dismiss the suit. In *Halkin I*, plaintiffs "succeeded in obtaining a limited amount of discovery," *id.*, 598 F.2d at 4-5, before a number of plaintiffs' claims were dismissed. In *Halkin II*, "[a] large number of documents responsive to plaintiffs' [discovery] requests were produced." *Id.*, 690 F.2d at 984. In addition, the CIA identified various plaintiffs who were surveilled and specified to some degree how they were surveilled. *Id.* at 985 n.28.

In both *Halkin I & II*, the court (which, again, did not have the benefit of *Webster*) applied *Reynolds* and refused to balance plaintiffs' interests in disclosure with the government's interest in protecting national security. *Halkin II*, 690 F.2d at 990. Dissenting from the court's denial of the petition for rehearing *en banc*, Judges Bazelon and Wright wrote that "[o]nly a total disregard for the importance of the Fourth Amendment interest could lead the panel to decide this case without first considering" the *Keith* case, and accused the panel of "us[ing] the evidentiary privilege to immunize conduct that appears to be proscribed by the Fourth Amendment." *Halkin I*, 598 F.2d at 13.

The dissenters were, of course, largely vindicated in *Webster*, which limited the *Reynolds* test and required courts to "balance [plaintiffs'] need for access to proof which would support a colorable constitutional claim" against the "extraordinary" security needs of the government to protect, *inter alia*, "methods, sources, and mission." *Webster*, 486 U.S. at 604. Another case that did not have the benefit of *Webster* was *Ellsberg v. Mitchell*, 709 F.2d 51 (D.C. Cir. 1983). There, former defendants and attorneys in the "Pentagon Papers" case brought a damage action against persons who allegedly subjected them to warrantless electronic surveillance. The government provided substantial discovery, identifying a number of the plaintiffs who had been wiretapped and where the surveillance occurred, *id.* at 53-55, but refused on state secrets grounds to answer other interrogatories. On appeal, the D.C. Circuit ordered the government to provide the names of the persons who authorized the wiretaps, but refused to order other (undisclosed) discovery to plaintiffs. *Id.* at 59-60. The court did not dismiss claims concerning wiretaps the government had conceded, "see[ing] no reason . . . to suspend the general rule that the burden is on those seeking an exemption from the Fourth Amendment

warrant requirement to show the need for it.” *Id.* at 68. The court, however, did dismiss the claims of persons for whom wiretapping was not conceded. *Id.* at 65.

Halkin I, *Halkin II*, and *Ellsberg* did not have the benefit of the Supreme Court’s teaching in *Webster*, that—at least where constitutional claims are at issue—courts *should* “balance [plaintiffs’] need for access to proof which would support a colorable constitutional claim” against the “extraordinary” security needs of the government to protect, *inter alia*, “methods, sources, and mission.” 486 U.S. at 604. Nor did they involve a statute, such as FISA, that “contemplat[es] the trial of actions that by their very nature concern security information.” *Halpern*, 258 F.2d at 44. This court should therefore apply the Supreme Court opinion in *Webster*, and the relevant Second Circuit opinion in *Halpern*, not the outdated (and in any event, non-controlling) precedent from the D.C. Circuit.

C. The State Secrets Privilege Does Not Apply to a Massive, Illegal Program That Reaches Into the Heartland of This Country and Violates The Constitutional Rights of Millions of Ordinary Americans

Even if FISA did not preempt the state secrets privilege, which it plainly does, *see supra* § II(A), this case cannot be dismissed at the pleading stage for four additional, independent reasons: (1) By its own terms, the state secrets privilege does not apply to this case; (2) *Webster*, not *Reynolds*, controls when constitutional claims are at stake, and *Webster* requires balancing of the parties’ interests, not dismissal; (3) *Reynolds*, which was decided in a considerably different factual context, does not require dismissal; and (4) defendants’ actions are not secret, and therefore not “state secrets.”

1. Because This Case Concerns Civilian, not “Military Matters,” the State Secrets Privilege Does Not Apply

As this Court observed in *Hepting*, “most cases in which the very subject matter [of the case] was a state secret involved classified details about either a highly technical invention or a covert espionage relationship.” *Id.*, 439 F.Supp.2d at 993. There is good reason for this. The *Reynolds* holding, by its own terms, dealt *only* with “military matter[s].” 345 U.S. at 10 (privilege applies *only* where “there is a reasonable danger that compulsion of the evidence will expose *military matters* which, in the interest of national security, should not be divulged.”). The secret test flight of a B-29 bomber (*Reynolds*), the covert spy relationships with President Lincoln (*Totten*) and with the CIA (*Tenet*), and operations on an Air Force base (*Kasza*), are all plainly core “military matters.”²¹ But if *Youngstown Sheet* teaches anything, it is that the encroachment of the military into the purely *civilian* affairs of ordinary Americans, e.g., spying

²¹The great majority of state secrets cases similarly concern core military matters and/or persons who worked with or for United States intelligence or the military. *See, e.g., Sterling v. Tenet*, 416 F.3d 338 (4th Cir. 2005) (CIA covert agent’s employment lawsuit against CIA); *Edmonds v. United States Dept. of Justice*, 323 F.Supp.2d 65 (D.D.C. 2004) (action by terminated FBI employee); *Tilden v. Tenet*, 140 F.Supp.2d 623 (E.D.Va. 2000) (CIA employee suit against CIA); *Bareford v. General Dynamics Corp.*, 973 F.2d 1138 (5th Cir. 1992) (defective weapon causing death of sailors in Iraqi missile attack); *Zuckerbraun v. General Dynamics Corp.*, 935 F.2d 544 (2nd Cir. 1991) (malfunction of missile defense system aboard U.S. Navy frigate); *In re Under Seal*, 945 F.2d 1285 (4th Cir. 1991) (action by government contractor for failure to renew contract involving “highly-classified program”); *Department of Navy v. Egan*, 484 U.S. 518 (1988) (denial of security clearance to Trident Naval Refit Facility, which services Trident nuclear weapons); *Fitzgerald v. Penthouse Int’l, Ltd.*, 776 F.2d 1236 (4th Cir. 1985) (Navy and CIA “dolphin torpedo” and “open-ocean weapons systems”); *Molerio v. FBI*, 749 F.2d 815 (D.C. Cir. 1984) (FBI refusal to hire plaintiff as a special agent); *Northrop Corp. v. McDonnell Douglas Corp.*, 751 F.2d 395 (D.C. Cir. 1984) (defense contractor subpoena of Department of Defense concerning sale of military equipment to foreign countries); *Military Audit Project v. Casey*, 656 F.2d 724 (D.C. Cir. 1981) (FOIA request concerning secret CIA project to raise sunken Russian submarine from the Pacific Ocean floor); *Farnsworth Cannon, Inc. v. Grimes*, 635 F.2d 268 (4th Cir. 1980) (action by Navy contractor against Navy employee for loss of Navy contract) (cases all cited by defendants).

upon hundreds of millions of phone calls and emails that have *nothing* to do with the military or with foreign intelligence, is a *civilian* matter. *Id.*, 343 U.S. at 587; *id.* at 642 (Jackson, J., concurring) (“[N]o doctrine that the Court could promulgate would seem . . . more sinister and alarming than that a President . . . can vastly enlarge his mastery over the internal affairs of the country by his own commitment of the Nation’s armed forces to some foreign venture.”); *id.* at 644 (“The military powers of the Commander-in-Chief were not to supersede representative government of internal affairs Congress, not the Executive, should control utilization of the war power as an instrument of domestic policy.”); *id.* at 632 (Douglas, J., concurring) (“[O]ur history and tradition rebel at the thought that the grant of military power carries with it authority over civilian affairs.”); *Al-Marri*, 2007 WL 1663712, at *28 (“[I]n this nation, military control cannot subsume the constitutional rights of civilians.”).

Were it otherwise, there is *nothing* the military could not do within the wide landscape of this country that could not be cloaked by the state secrets privilege. If, for example, the military secretly took over the nation’s entire telecommunications network in order to monitor Al Qaeda, revelation of this program (which might tip off Al Qaeda) could arguably impair national security. If the military secretly took over the broadcast networks in order to control the airwaves, suppress pro-Al Qaeda news stories, and spread anti-Al-Qaeda propaganda, revelation of this program (which would damage the credibility of the propaganda) could also impair national security. Even though these Executive actions would violate the Constitution, *see Youngstown Sheet*, they could not be revealed much less enjoined, because revelation of just about *any* program involving the military—no matter how invasive of domestic affairs or obnoxious to the Constitution—could arguably impair national security.

Thankfully *Reynolds* precludes such plainly absurd results. *Reynolds* carefully included only purely “military matters” within its holding. It did not invite the government to extend the state secrets privilege into the civilian arena, and for good reason. We have long enjoyed a “deeply rooted and ancient opposition in this country to the extension of military control over civilians,” *Reid*, 354 U.S. at 33, and to “any military intrusion into civilian affairs.” *Laird*, 408 U.S. at 15. Extension of the state secrets privilege to conceal and essentially sanction such “military intrusion,” *id.*, would run head first into this ancient and vital constitutional doctrine. *See id.*; *Youngstown Sheet*, 343 U.S. at 587.

Reynolds dealt with a limited and traditional application of the state secrets privilege, one confined to a purely “military matter”: the secret flight of a B-29 bomber. *Reynolds* therefore carefully limited the privilege (and its holding) to “military matters.” The state secrets privilege does not apply in this case, *see id.*, nor could it, *see Reid*, 354 U.S. at 33; *Laird*, 408 U.S. at 15; *Youngstown Sheet*, 343 U.S. at 587.²²

2. The Supreme Court Case in *Webster* Requires Balancing of the Parties’ Interests, not Dismissal

Even if the eavesdropping of hundreds of millions of private conversations and emails between parents and their children, between spouses, co-workers, friends, doctors,

²²This is not to say that the Executive has no interest at all in maintaining the confidentiality of some aspects of the Dagnet program. But such interests can be accommodated by more traditional remedies, *see, e.g., Webster*, 486 U.S. at 603, and, in any event, do not trump this Court’s “province and duty. . . to say what the law is,” *Marbury*, 5 U.S. at 177, nor plaintiffs’ interests in vindicating their rights under the Fourth Amendment and three separate federal statutes.

teachers, accountants, judges, the clergy, *et al.* were somehow a “military matter,” the state secrets privilege would not require dismissal of this case.

Where constitutional claims are at stake, Supreme Court precedent requires a balancing of the parties’ interests, not dismissal. *Reynolds* did not involve constitutional claims. *Reynolds* instead involved a tort case brought by three people, involving no issues of constitutional significance. *Kasza* was also a tort case, involving no constitutional claims. In contrast, this class action on behalf of hundreds of millions of Americans involves arguably the most sweeping violation of constitutional rights by a President in the nation’s history. As this Court previously noted, “no case dismissed because its ‘very subject matter’ was a state secret involved ongoing, widespread violations of individual constitutional rights.” *Hepting*, 439 F.Supp.2d at 993.

This is significant. Here defendants seek to use a common law privilege to deny plaintiffs a judicial forum to assert their Fourth Amendment right to be free from a Dragnet surveillance program. But as the Supreme Court held in *Webster*, a case that post-dates *Reynolds*, a “serious constitutional question . . . would arise” if even “a federal *statute* were construed to deny any judicial forum for a colorable constitutional claim.” *Webster*, 486 U.S. at 603 (citation omitted). In *Webster*, the plaintiff (unlike Plaintiffs here) did contract with and work for the United States (in the CIA). Notwithstanding plaintiff’s status as a former CIA employee, and notwithstanding the CIA Director’s claim that “judicial review even of [plaintiff’s] constitutional claims” will be “to the detriment of national security,” *id.* at 604, the Supreme Court refused to dismiss the case. Instead, and in contrast to *Reynolds* (which involved no constitutional claim), the Court instructed the district court to “balance [plaintiff’s] need for

access to proof which would support a colorable constitutional claim against the extraordinary needs of the CIA for confidentiality and the protection of its methods, sources, and mission.” *Id.*; *see also Stehney v. Perry*, 101 F.3d 925, 934 (3rd Cir. 1996) (permitting plaintiff to mount constitutional challenge to the NSA’s revocation of her national security clearance in part to avoid the “serious constitutional question that would arise if a federal statute were construed to deny any judicial forum for a colorable constitutional claim”).

Defendants ask the Court to deny plaintiffs a judicial forum to vindicate their Fourth Amendment rights. That *Webster* does not permit. The *Webster* court was familiar with *Reynolds*. It cited *Reynolds*. But the *Webster* court struck a different balance where constitutional rights were at stake—permitting the case to proceed, discovery to be held, and a careful balancing of the parties’ respective interests.

This case is even stronger than *Webster*, because Congress passed a law (FISA) authorizing discovery, not requiring dismissal. The constitutional interests at stake here are also far greater than in *Webster*. *Webster* involved a single plaintiff, asserting fairly weak constitutional claims.²³ *Shubert* is a putative class of millions of Americans, asserting extremely serious violations of the Fourth Amendment. Defendants’ radical attempt to deny plaintiffs a judicial forum to assert their Fourth Amendment claims must be rejected. *Webster*, 486 U.S. at 603.²⁴

²³*See Webster*, 486 U.S. at 602 (“We share the confusion of the Court of Appeals as to the precise nature of respondent’s constitutional claims.”).

²⁴*El-Masri v. Tenet*, 479 F.3d 296 (4th Cir. 2007), cited by defendants, failed even to cite *Webster*, much less distinguish it. *El-Masri* is also inapposite because it did not involve a statute “contemplating the trial of actions that by their very nature concern security information,” *Halpern*, 258 F.2d at 44, *see supra* § II(A); nor a program already largely “in the public record,”

3. ***Reynolds*, Which Was Decided In a Considerably Different Factual Context, Does Not Require Dismissal**

Reynolds is distinguishable in at least five further respects. First, *Reynolds* involved persons who volunteered to go on a plainly military mission. *Totten*, *Tenet*, and *Kasza* all involved persons working for the military. But plaintiffs here did not join, observe, contract with, or spy for the United States military or a United States intelligence agency. The named plaintiffs did not. The putative plaintiff class did not. Plaintiffs are ordinary Americans, as far removed from the United States military and intelligence establishment as is possible in any case.

In *Reynolds*, there was no reason even to believe that the withheld information implicating state secrets “had any causal connection with the accident.” 345 U.S. at 11. The secret electronic equipment in that case was irrelevant to prove the plaintiffs’ case. In contrast, defendants here seek not only to withhold all discovery (including any and all discovery they have relevant to plaintiffs’ case), they seek to dismiss the case entirely.

In *Reynolds*, defendants “formally offered to make the surviving crew members available for examination,” an offer plaintiffs rejected but that the Supreme Court believed “should have been accepted.” *Id.* Whatever minimal harm was caused to plaintiffs’ case by the failure to produce an irrelevant report on the electronic equipment was more than minimized by the government’s offer to produce live witnesses. This case stands in stark contrast. The

Hepting, 439 F.Supp.2d at 994, *see infra* § II(C)(4). In addition, *El-Masri*, which dealt with the detention of a foreign citizen in a foreign country, did not concern a military intrusion into domestic American affairs. *See Youngstown Sheet*, 343 U.S. at 587; *Al-Marri*, 2007 WL 1663712. *El-Masri* also concluded that a single plaintiff’s “personal interest in pursuing his civil claim is subordinated to the collective interest in national security.” *Id.* at 313. Here the collective interest of millions of Americans in preserving both FISA and the Fourth Amendment throughout the United States is at least as great as the security interest asserted by defendants.

withheld discovery (*i.e.*, *all* discovery) is extremely relevant, and defendants have provided no alternative: no witnesses, no documents, nothing at all besides a demand for dismissal.

Unlike *Reynolds* (but like *Youngstown Sheet*), this case involves a startling encroachment of the Executive into the domestic sphere. The Dragnet program monitors, intercepts, and searches the contents of hundreds of millions of phone calls and emails made within the United States, calls by ordinary Americans to their family, friends, and others. Compl. ¶¶ 1-3, 53-90. The Dragnet program is far more intrusive within the domestic sphere than President Truman's unconstitutional actions, which affected a limited number of steel mills. *Reynolds* simply had no occasion to consider the privilege within such a context.

Unlike *Reynolds* (but like *Al-Marri*, 2007 WL 1663712), this case also involves a "military intrusion into civilian affairs." *Laird*, 408 U.S. at 15. This is no minor intrusion, but—as alleged—the most widespread and substantial "military intrusion into civilian affairs" since the Civil War. The National Security Agency, which is the intelligence arm of the Department of Defense, is now engaged in a national electronic quartering program, monitoring the daily lives of millions of ordinary Americans: their conversations, their email, their internet use. *Reynolds*, which dealt with secret electronic equipment on a military aircraft, again had no occasion to consider the privilege in this context.

"[E]ven the state secrets privilege has its limits." *Hepting*, 439 F.Supp.2d at 995. The privilege as defined in *Reynolds* applies *only* to "military matters," but the Dragnet surveillance of millions of phone calls and emails by ordinary Americans within this country is a civilian matter, not a military one. The test set forth in *Reynolds* does not and cannot apply where, as here, constitutional rights are at stake. *See Webster*, 486 U.S. at 603. Rather, courts

have “latitude to control any discovery process which may be instituted so as to balance [plaintiffs’] need for access to proof which would support a colorable constitutional claim against the extraordinary needs of the [government] for confidentiality and the protection of its methods, sources, and mission.” *Id.* at 604.

The Court in *Reynolds*, in that limited, straightforward case, could not possibly have imagined that any executive would so misuse the state secrets privilege, as to attempt to apply it to sweeping, criminal, unconstitutional conduct reaching into the heartland of this country. As this Court noted, “While the court recognizes and respects the executive’s constitutional duty to protect the nation from threats, the court also takes seriously its constitutional duty to adjudicate the disputes that come before it To defer to a blanket assertion of secrecy here would be to abdicate that duty.” *Hepting*, 439 F.Supp.2d at 995 (citation omitted).

Just as “[t]he President cannot eliminate constitutional protections with the stroke of a pen by proclaiming a civilian, even a criminal civilian, an enemy combatant subject to indefinite military detention,” *Al-Marri*, 2007 WL 1663712, at *27, the President’s intelligence chief cannot, with the stroke of a declaration, conceal and effectively immunize a criminal Dagnet program that subjects hundreds of millions of ordinary Americans to round-the-clock surveillance by the United States military. “For a court to uphold a claim to such extraordinary power would do more than render lifeless” the Fourth Amendment, plaintiffs’ right to a judicial forum, the constitutional right and duty of Article III courts to “say what the law is,” *Marbury*, 5 U.S. at 177, and fundamental constitutional limitations upon the Executive within the domestic

sphere, *see Youngstown Sheet*, 343 U.S. at 587. “[I]t would effectively undermine all of the freedoms guaranteed by the Constitution.” *Al-Marri*, 2007 WL 1663712, at *29.

The Executive offers no limiting principle—*none*—for its breathtaking extension of the state secrets privilege. In defendants’ view, *any* illegal conduct, *any* unconstitutional conduct, *any* violation of law—no matter how many people it affects, no matter how violative it is of fundamental rights—cannot be stopped, or even revealed, so long as revelation of the conduct might harm national security. Even a secret program to put a camera in every American’s bedroom could not be revealed, if to reveal it might harm national security. But the Executive cannot transform a limited evidentiary privilege into *de facto* executive immunity for violations of the Constitution and federal criminal laws. Such an awesome power “either has no beginning or it has no end. If it exists, it need submit to no legal restraint. . . . [It may not] plunge us straightway into dictatorship, but it is at least a step in that direction.” *Youngstown Sheet*, 343 U.S. at 653 (Jackson, J., concurring).

4. **Because the Content Monitoring Program Is Not Secret, It Is Not a “State Secret”**

Defendants’ motion should be denied for yet another reason. As this Court previously held, defendants’ content monitoring program is “hardly a secret,” much less a “state secret.” *Hepting*, 439 F.Supp.2d at 994. Defendants publicly “admitted the existence” of the program, that it “monitor[s] communication content,” “tracks calls into the United States or out of the United States,” and “operates without warrants.” *Id.* at 992 (citations omitted). Because the “very subject matter of this action is hardly a secret,” the state secrets privilege cannot bar this suit. *Id.* at 994; *see also Jencks v. United States*, 353 U.S. 657, 675 (1957) (Burton, J.,

concurring) (“Once the defendant learns the state secret . . . the underlying basis for the privilege disappears, and there usually remains little need to conceal the privileged evidence from the jury. Thus, when the Government is a party, the preservation of these privileges is dependent upon nondisclosure of the privileged evidence to the defendant.”).

The Executive has also “opened the door for judicial inquiry by publicly confirming and denying material information about its monitoring of communication content.” *Hepting*, 439 F.Supp.2d at 996. Defendants cannot *both* deny the existence of a broader Dragnet, *and* claim that the state secrets privilege prevents them from making such a denial. Yet that is what the Executive does here. In support of this motion, defendants submitted a declaration from Keith Alexander, Director of the National Security Agency, swearing that “Plaintiffs’ allegations of a content surveillance dragnet are false.” *See* Public Alexander Declaration, May 25, 2007 ¶ 16. “If the government’s public disclosures have been truthful,” discovery regarding those disclosures “should not reveal any new information that would assist a terrorist and adversely affect national security.” But “if the government has not been truthful, the state secrets privilege should not serve as a shield for its false public statements.” *Hepting*, 439 F.Supp.2d at 996.²⁵ The existence of defendants’ warrantless content surveillance program is plainly not subject to the state secrets privilege.

D. The *Totten/Tenet* Bar Does Not Apply

Both *Totten* and *Tenet* dealt with the disclosure of secret espionage relationships. Plaintiffs are not spies, “made no agreement with the government and are not bound by any

²⁵Were it otherwise, the state secrets privilege would simply be a license for government officials to lie.

implied covenant of secrecy.” *Hepting*, 439 F.Supp.2d at 991; *cf. Totten*, 92 U.S. at 106; *see also Tenet*, 544 U.S. at 10 (further restricting narrow *Totten* rule to suits brought by “alleged former sp[ies],” not to “acknowledged (though covert) employee[s] of the CIA”). For the reasons set forth in *Hepting*, the narrow *Totten/Tenet* bar is irrelevant to this case.

III. Defendants’ Standing Argument Is a Red Herring

For the reasons set forth in *Hepting*, defendants’ attempt to dismiss this case on standing grounds should be rejected. *See id.*, 439 F.Supp.2d at 999-1001. “[T]he core component of standing is an essential and unchanging part of the case-or-controversy requirement of Article III.” *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992). A plaintiff must satisfy three elements to have standing: (1) “the plaintiff must have suffered an injury in fact—an invasion of a legally protected interest which is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical”; (2) “there must be a causal connection between the injury and the conduct complained of”; and (3) “it must be likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision.” *Id.* at 560-61 (internal quotation marks and citations omitted).

The Complaint plainly alleges all three elements.²⁶ The “President of the United States authorized a secret program to spy upon millions of innocent Americans, including the

²⁶“For purposes of ruling on a motion to dismiss for want of standing, both the trial and reviewing courts must accept as true all material allegations of the complaint, and must construe the complaint in favor of the complaining party.” *Wilbur*, 423 F.3d at 1107 (citation omitted). In addition, “[a]t the pleading stage, general factual allegations of injury resulting from the defendant’s conduct may suffice, for on a motion to dismiss we presume that general allegations embrace those specific facts that are necessary to support the claim.” *Lujan*, 504 U.S. at 561 (citation and internal quotation marks omitted).

named plaintiffs.” *Id.* ¶ 2. The program “intercept[ed], search[ed], seiz[ed], and subject[ed] to surveillance the content of [their] personal phone conversations and email.” *Id.* The program has operated and continues to operate “without a warrant, court order or any other lawful authorization.” *Id.* ¶ 1. The named plaintiffs have been and continue to be spied upon illegally pursuant to the program. *Id.* ¶¶ 5-8.²⁷ “Plaintiffs are ‘aggrieved person[s]’ as defined in 50 U.S.C. § 1810, are not foreign powers or agents of a foreign power, and were subjected to electronic surveillance conducted or authorized by defendants pursuant to the Spying Program in violation of 50 U.S.C. § 1809,” *id.* ¶ 98, and are therefore entitled to damages under 50 U.S.C. § 1810 (FISA). Plaintiffs are also alleged to be “aggrieved persons” as defined by the Wiretap Act and the Stored Communications Act, and are entitled to damages pursuant to those statutes. *Id.* ¶¶ 102-108. Finally, “by conducting, authorizing, and/or participating in the electronic surveillance of plaintiffs, and by searching and seizing the contents of plaintiffs’ communications without reasonable suspicion or probable cause, and failing to prevent their fellow government officers from engaging in this unconstitutional conduct, defendants deprived plaintiffs of rights, remedies, privileges, and immunities guaranteed under the Fourth Amendment of the United States Constitution.” *Id.* ¶ 110.

In short, plaintiffs (1) were illegally spied upon and are being spied upon (2) by defendants and are (3) entitled to damages. Should the Court enjoin defendants’ illegal program, the Court will also redress an ongoing legal violation directly traceable to defendants, that will prevent further injury to plaintiffs. These allegations plainly establish standing, and defendants do not suggest otherwise. *See American Civil Liberties Union v. National Security Agency*, 2007

²⁷Further aspects of the program are set forth in paragraphs 53-90 of the Complaint.

WL 1952370, at *5 (6th Cir. July 6, 2007) (“If . . . a plaintiff could demonstrate that her privacy had actually been breached (i.e., that her communications had actually been wiretapped), then she would have standing to assert a Fourth Amendment cause of action for breach of privacy.”); Defendants’ Memorandum of Law dated May 26, 2007 (“Def. Br.”), at 26 (conceding that “aggrieved persons” as defined by FISA, the Wiretap Act, and the Stored Communications Act have standing to assert violations of those statutes); *Director, Office of Workers’ Comp. Programs v. Newport News Shipbuilding & Dry Dock Co.*, 514 U.S. 122, 126 (1995) (“aggrieved” is a well-known term of art used to “designate those who have standing”) (cited by defendants at Def. Br. 26).²⁸

To the contrary, defendants *concede* that plaintiffs have alleged standing. As defendants put it, “persons whose rights were injured by the actual interception or disclosure of their own communications (or records) have standing.” Def. Br. 26. Defendants instead are reduced to claiming that plaintiffs will not ultimately be able, at some future time, to *prove* standing because of the state secrets privilege. The standing argument is no more than state secrets revisited, and for all the reasons set forth in section II, *supra*, the argument fails. “[T]he state secrets privilege will not prevent plaintiffs from receiving at least some evidence tending to establish the factual predicate for the injury-in-fact underlying their claims.” *Hepting*, 439

²⁸As in *Hepting*, “the gravamen of plaintiffs’ complaint is that [defendants] created a dragnet” that collected the content of plaintiffs’ communications. *Hepting*, 439 F.Supp.2d at 1000. “[T]he alleged injury is concrete even though it is widely shared. Despite [defendants’] alleged creation of a dragnet to intercept all or substantially all of [plaintiffs’] communications, this dragnet necessarily inflicts a concrete injury that affects each [plaintiff] in a distinct way.” *Id.* at 1001 (citing *FEC v. Akins*, 524 U.S. 11, 24 (1998) (“[W]here a harm is concrete, though widely shared, the Court has found ‘injury in fact.’”)).

F.Supp.2d at 1001.²⁹ In addition, “additional facts might very well be revealed during, but not as a direct consequence of, this litigation that obviate many of the secrecy concerns currently at issue” regarding the program and therefore “it is unclear whether the privilege would necessarily block [defendants] from revealing information” about the program. *Id.* Finally, for the many other reasons set forth in Section II, *supra*, the state secrets privilege does not apply and, even if it did, will not bar plaintiffs from establishing the factual predicate for the injury-in-fact underlying their claims.

A. The Sixth Circuit Opinion in *ACLU v. NSA* Does Not Help Defendants

Defendants will undoubtedly attempt to rely upon the recent opinions in *American Civil Liberties Union v. National Security Agency*, 2007 WL 1952370 (6th Cir. July 6, 2007), which dismissed the ACLU’s limited challenge to the TSP on standing grounds. *ACLU* is irrelevant to this case for a number of reasons.³⁰

ACLU turned on a number of factors not present here. First, the case presented a “relatively unique procedural posture”: plaintiffs moved for partial summary judgment based on a statement of undisputed facts and defendants cross-moved for summary judgment. Because, on a motion for summary judgment, “the plaintiff can no longer rest on mere allegations” (as they

²⁹In light of the many admissions by, *inter alia*, the President, the Attorney General, and General Hayden, and the Klein and Marcus declarations noted in *Hepting*, 439 F.Supp.2d at 1001, there is “at least some factual basis for plaintiffs’ standing,” *id.*, and it is absurd for defendants to suggest that this case is a “groundless fishing expedition.” Def. Br. at 33.

³⁰As a preliminary matter, the opinion of Judge Batchelder is of little precedential value, because the concurring judge concurred only in the judgment and the concurrence is more narrow than Judge Batchelder’s opinion. See *Panetti v. Quarterman*, 127 S.Ct. 2842, 2856 (2007) (“When there is no majority opinion, the narrower holding controls.”).

can do at the pleading stage) “but must set forth by affidavit or other evidence specific facts,” *Lujan*, 504 U.S. at 561 (internal quotation marks omitted), and because plaintiffs “failed to provide evidence that they are personally subject to the TSP,” the *ACLU* plaintiffs could not establish standing. *ACLU*, 2007 WL 1952370, at *34, 39.

Here, of course, plaintiffs have not moved for summary judgment, nor set forth a set of undisputed facts. Defendants’ motion comes at the pleading stage, before they have even answered.³¹ In this posture, “general factual allegations of injury resulting from the defendant’s conduct may suffice, for on a motion to dismiss we presume that general allegations embrace those specific facts that are necessary to support the claim.” *Lujan*, 504 U.S. at 561; *see Hepting*, 439 F.Supp.2d at 999 (same). There is no dispute that the factual allegations of injury set forth in the Complaint establish plaintiffs’ standing.

Second, in *ACLU*, “plaintiffs [did] not challenge[] the government’s invocation of the [state secrets] privilege or its application.” *ACLU*, 2007 WL 1952370, at *38 (concurrence). Based on this failure, both the concurrence and Judge Batchelder assumed, with little analysis, that the privilege applied and would have precluded plaintiffs (had they asked) from determining whether or not they were in fact surveilled. *Id.*

In contrast, plaintiffs here vigorously contest both the invocation of the state secrets privilege and its application. Plaintiffs do not concede that the state secrets privilege applies; rather, the FISA statute controls, *see supra* § II(A); the state secrets privilege does not by its own terms apply to this case, *see supra* § II(C)(1); *Webster* requires balancing of the parties’

³¹Defendants’ alternative “summary judgment” motion is also improper and premature. *See supra* n.7.

interests, and the provision of some discovery, *see supra* § II(C)(2); even if *Reynolds* applied, it would not preclude discovery further demonstrating plaintiffs' injury-in-fact, *see supra* § II(C)(3); and defendants' actions are not even secret, much less "state secrets," *see supra* § II(C)(4).

Third, the *ACLU* plaintiffs never alleged that they were surveilled; rather, they alleged that it was possible that they were surveilled, creating a "chilling effect" on their ability to communicate with their clients. While the Sixth Circuit panel was deeply divided as to whether this chilling effect was sufficient to create injury-in-fact,³² the debate is of no moment here, where plaintiffs alleged that they *have* been surveilled, many times, under defendants' Dragnet program. *See, e.g.*, Compl. ¶¶ 1-2, 5-8. As defendants concede, a plaintiff who has been surveilled unquestionably has standing to challenge the surveillance. Def. Br. 26.

Fourth, the *ACLU* plaintiffs only sought injunctive relief, not damages. To the extent Judges Batchelder and Gibbons believed that any future surveillance of plaintiffs was speculative, they ruled that the request for injunctive relief was precluded by *City of Los Angeles v. Lyons*, 461 U.S. 95 (1983), which held that a purely speculative fear of future injury (there, the fear of a future arrest and choke hold by some hypothetical, future police officer in violation of city policy) did not create standing to request prospective injunctive relief. *Lyons*, though, is of

³²*Cf. ACLU*, 2007 WL 1952370, at *36 ("[A] plaintiff must be actually subject to the defendant's conduct, not simply afraid of being subject to it"); *id.* at *45 ("All that was required was that they demonstrate that . . . they possessed a reasonable fear of harm The existence of the TSP is undisputed and these plaintiffs are personally affected by the TSP whether they engage in targeted communications or not.") (Gilman, J., dissenting). In the Ninth Circuit, Judge Gilman's dissenting view would plainly have prevailed. *See The Presbyterian Church (U.S.A.) v. United States*, 870 F.2d 518, 521-22 (9th Cir. 1989) (Church has standing where fear of surveillance chilled congregants from participating in church services).

no relevance to claims that assert damages. *Id.* In addition, plaintiffs here (unlike plaintiffs in *ACLU*) allege that they are *currently* subject to an existing, ongoing Dragnet program, and will continue to be subject to the program until the program is enjoined by a federal court.

Finally, in *ACLU* the government argued that, because plaintiffs there *did* communicate with Al Qaeda suspects, the warrantless TSP could not chill those conversations, because they would have been monitored with or without a FISA warrant.³³ The argument is of no relevance here. Plaintiffs—millions of ordinary Americans—do not communicate with Al Qaeda and are not agents of a foreign government. No FISA court would provide defendants a warrant to spy upon hundreds of millions of phone conversations and emails by and between ordinary Americans. *See* 50 U.S.C. § 1801 *et seq.* (setting forth requirements for FISA warrant). If the Court were to enjoin the Dragnet, the Dragnet would end and plaintiffs would no longer be subject to *any* surveillance. The ongoing harm to plaintiffs—a startling loss of privacy of unprecedented scope—would plainly be redressed by an injunction to stop the Dragnet program.

At the pleading stage, plaintiffs have established standing. Defendants' motion should be denied.³⁴

³³This analysis is flawed for the many reasons set forth in Plaintiffs' Supplemental Memorandum in *Center for Constitutional Rights v. Bush*, Case No, 07-1115, dated July 9, 2006, at 16-17.

³⁴In a footnote, defendants suggest that the United States has not waived sovereign immunity for damages under the statutes at issue here. Motions made in a footnote are waived. *See, e.g., Hilao v. Estate of Marcos*, 103 F.3d 767, 778 n.4 (9th Cir. 1996); *see also Retlaw Broadcasting Co. v. N.L.R.B.*, 53 F.3d 1002, 1005 n.1 (9th Cir. 1995). In any event, defendants are wrong. FISA explicitly and unequivocally waives sovereign immunity. It provides a cause of action for damages against any "person" who commits unlawful electronic surveillance in violation of 50 U.S.C. § 1809. FISA defines a "person" to include "any officer or employee of the Federal Government." 50 U.S.C. § 1801(m). An action against federal officers and employees in their official capacities "is considered a suit against the United States." *Multi*

IV. Defendants' Statutory Arguments Fail

A. Neither Statute Requires Dismissal

Defendants' statutory arguments also fail. Defendants now concede, as they must, that neither Section 6 of the National Security Act of 1959, 50 U.S.C. § 402 note, nor Section 102A(i)(1) of the Intelligence Reform and Terrorism Prevention Act of 2004, 50 U.S.C. § 403-1(i)(1), requires dismissal. *See* Def. Br. 38 ("The Court observed that 'neither [statute] requires the court to dismiss this action.' That is true.") (citing *Hepting*).

The concession disposes of the argument. "Neither of these provisions by their terms requires the court to dismiss this action and it would be premature for the court to do so at this time." *Hepting*, 439 F.Supp.2d at 998; *see Al-Haramain*, 451 F.Supp.2d at 1227 (denying the government's motion to dismiss on the basis of the statutory provisions: "[t]he statutory privileges at issue here do not direct the dismissal of this action, nor am I yet convinced that they

Denominational Ministry v. Gonzales, 474 F.Supp.2d 1133, 1140 (N.D.Cal. 2007). By prescribing civil damages liability for FISA violations by federal officers or employees, and hence the United States, FISA waives federal sovereign immunity. *See Salazar v. Heckler*, 787 F.2d 527, 529 (10th Cir. 1986) (Title VII of Civil Rights Act of 1974, which authorized civil actions for employment discrimination by specifying "the head" of an offending federal entity as defendant, *see* 42 U.S.C. § 2000e-16(c), waives sovereign immunity despite failure to specify "the United States"); *Rochon v. Gonzales*, 438 F.3d 1211, 1215-16 (D.C. Cir. 2006) (same).

FISA also waives sovereign immunity because it defines "person" to include any "entity," *without excepting the United States*, as do, for example, provisions of the Electronic Communications Privacy Act (ECPA). *See* 18 U.S.C. § 2520 (authorizing cause of action against a "person or entity, other than the United States"), § 2707(a) (same). "Entity" includes "governmental entities" such as the United States. *See Organizacion JD Ltda v. U.S. Dept. Of Justice*, 18 F.3d 91, 94 (2nd Cir. 1994) (in former ECPA: "person or entity" includes "governmental entity"); *Adams v. City of Battle Creek*, 250 F.3d 980, 985 (6th Cir. 2001) (same). Had Congress meant to except "the United States" from the scope of the word "entity" in section 1801(m), Congress could and would have done so.

will block evidence necessary to plaintiffs' case."). Both statutes are simply irrelevant to the motion.

At best for defendants, these statutes may or may not be relevant to disputes that later arise in discovery. *See Hepting*, 439 F.Supp.2d at 998 ("After discovery begins, the court will determine step-by-step whether the privileges prevent plaintiffs from discovering particular evidence. But the mere existence of these privileges does not justify dismissing this case now."); *Al-Haramain*, 451 F.Supp.2d at 1227 ("In proceeding with the discovery process, the government is free to identify discovery requests that fall within these other statutory privileges, and explain specifically why this is so, and I will determine whether the privileges prevent plaintiffs from discovering that specific evidence."); *Founding Church of Scientology v. NSA*, 610 F.2d 824, 833 (D.C. Cir. 1979) (authorizing discovery to develop "the basis for nondisclosure or the lack of it").

B. FISA Supplants the Statutory Provisions

The general statutes cited by defendants are also trumped in this case by the specific FISA statute. Section 6 of the National Security Act of 1959 was enacted twenty years prior to FISA and involves the NSA's general authority to withhold certain information (concerning the "organization or any function of the National Security Agency") from public disclosure. 50 U.S.C. § 402 note. FISA is a later, more specifically drawn statute that directly addresses electronic surveillance, the subject matter of this case. "[A] more specific statute will be given precedence over a more general one." *Busic v. United States*, 446 U.S. 398, 406 (1980); *Food & Drug Admin. v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120, 143 (2000) ("At the time a statute is enacted, it may have a range of plausible meanings. Over time, however,

subsequent acts can shape or focus those meanings This is particularly so where the scope of the earlier statute is broad but the subsequent statutes more specifically address the topic at hand. . . . [A] specific policy embedded in a later federal statute should control our construction of the [earlier] statute, even though it ha[s] not been expressly amended.”) (internal quotation marks and citations omitted).

Similarly, Section 102A(i)(1)’s generalized directive to the Director of the National Intelligence to protect intelligence sources and methods from unauthorized disclosure cannot overcome FISA’s more detailed provisions. FISA’s specific and relevant directives, concerning the precise subject matter of this action, prevail over Section 102(A)(i)(1) and control the outcome of this action. *See Basic*, 446 U.S. at 406.³⁵

C. On Its Face, Section 102(a)(i)(1) Applies to the DNI, Not to the Court

Section 102A(i)(1) provides: “The Director of National Intelligence shall protect intelligence sources and methods from unauthorized disclosure.” This section does no more than “instruct[] the Director of National Intelligence to take measures that are available to prevent disclosure regarding intelligence sources and methods—for example, by asserting the state secrets privilege.” *Terkel v. AT&T Corp.*, 441 F.Supp.2d 899, 906 (N.D.Ill. 2006). That has been done. On its face, this section requires no more. Its command is directed to the DNI and no one else.³⁶

³⁵Not one of the cases cited by defendants involved a FISA claim or the interplay between FISA and these two statutes.

³⁶The cases cited by defendants simply hold that the predecessor to Section 102A(i)(1) qualified as a “withholding statute” for purposes of Exemption 3 of the Freedom of Information Act. *See CIA v. Sims*, 471 U.S. 159, 167-68 (1985); *Fitzgibbon v. CIA*, 911 F.2d 755 (D.C. Cir. 1990). *Snapp v. United States*, 444 U.S. 507 (1980) does not concern either Section 102A(i)(1) or Section 6.

This section certainly does not require a court to abrogate its responsibility to adjudicate cases, nor to ignore the plain language of another statute specifically providing a discovery protocol where electronic surveillance is at issue. *See* 50 U.S.C. § 1806(f).

The DNI has presumably complied with this section and that is the end of this section's relevance to this case.

D. The Statutes Plainly Do Not Preclude Discovery From Third-Parties

Fourth, neither statute applies to discovery from third parties, such as the telecommunications providers who transferred the content of millions of phone and internet communications to the government. The cases cited by defendants apply (at best) only to direct discovery of the government, and then almost exclusively, to the unique interplay between FOIA and those statutes.³⁷ But discovery from third-parties will reveal substantial information in support of plaintiffs' claims.

E. Defendants' Interpretation of the Statutes Raises Serious Constitutional Concerns

Finally, defendants' reading of the statutes raises serious constitutional concerns. "[I]t would allow the federal government to conceal information regarding blatantly illegal or unconstitutional activities simply by assigning these activities to the NSA or claiming they implicated information about the NSA's functions." *Terkel*, 441 F.Supp.2d at 905; *see also Hayden*, 608 F.2d at 1389 (limiting Section 6 cases to where the NSA "function or activity is

³⁷*Sims*, 471 U.S. at 167-68 (CIA could withhold information under FOIA exemptions); *Founding Church*, 610 F.2d 824 (NSA could withhold information under FOIA exemptions); *Hayden v. NSA*, 608 F.2d 1381 (D.C. Cir. 1979) (same); *People for the Am. Way Found. v. NSA*, 462 F.Supp.2d 21 (D.D.C. 2006) (same)

authorized by statute and not otherwise unlawful)” (emphasis added). But a court should be “hard-pressed to read section 6 as essentially trumping every other Congressional enactment and Constitutional provision.” *Terkel*, 441 F.Supp.2d at 905. As the Supreme Court held in *Webster*, a “serious constitutional question . . . would arise if a federal statute were construed to deny any judicial forum for a colorable constitutional claim.” *Id.*, 486 U.S. at 603 (citation omitted).

The doctrine of constitutional avoidance also compels the Court not to adopt defendants’ reading. “If an otherwise acceptable construction of a statute would raise serious constitutional problems, and where an alternative interpretation of the statute is fairly possible, we are obligated to construe the statute to avoid such problems.” *Ramadan v. Gonzales*, 479 F.3d 646, 654 (9th Cir. 2007) (citation omitted). Reading Section 6 or Section 102A(i)(1) to preclude millions of Americans from asserting their Fourth Amendment right to be free from an electronic eavesdropping dragnet would, to put it mildly, “raise serious constitutional problems.” *Id.*; *Webster*, 486 U.S. at 603.

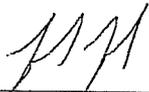
The Court, however, need not reach the doctrine of constitutional avoidance, because neither statute requires dismissal of the Complaint or of plaintiffs’ constitutional claims. “Neither of these provisions . . . requires the court to dismiss this action.” *Hepting*, 439 F.Supp.2d at 998.

CONCLUSION

For the foregoing reasons, plaintiffs respectfully request that this Court (1) determine that the Complaint states a valid legal claim; (2) deny defendants' motion in its entirety; and (3) grant such other relief as is just and proper.

Dated: July 19, 2007
New York, New York

EMERY CELLI BRINCKERHOFF
& ABADY LLP

By: 
Ilann M. Maazel
Matthew D. Brinckerhoff
Kennisha Austin

Attorneys for Plaintiffs

75 Rockefeller Plaza, 20th Floor
New York, New York 10019
(212) 763-5000