CINDY COHN (SBN 145997)
cindy@eff.org
LEE TIEN (SBN 148216)
KURT OPSAHL (SBN 191303)
JAMES S. TYRE (SBN 083117)
MARK RUMOLD (SBN 279060)
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco, CA 94110
Telephone: (415) 436-9333
Fax: (415) 436-9993

RACHAEL E. MENY (SBN 178514)
rmeny@kvn.com
PAULA L. BLIZZARD (SBN 207920)
MICHAEL S. KWUN (SBN 198945)
AUDREY WALTON-HADLOCK (SBN 250574)
KEKER & VAN NEST, LLP
633 Battery Street
San Francisco, CA 94111
Telephone: (415) 391-5400
Fax: (415) 397-7188

RICHARD R. WIEBE (SBN 121156)
wiebe@pacbell.net
LAW OFFICE OF RICHARD R. WIEBE
One California Street, Suite 900
San Francisco, CA 94111
Telephone: (415) 433-3200
Fax: (415) 433-6382

THOMAS E. MOORE III (SBN 115107)
tmoore@moorelawteam.com
THE MOORE LAW GROUP
228 Hamilton Avenue, 3rd Floor
Palo Alto, CA 94301
Telephone: (650) 798-5352
Fax: (650) 798-5001

ARAM ANTARAMIAN (SBN 239070)
aram@eff.org
LAW OFFICE OF ARAM ANTARAMIAN
1714 Blake Street
Berkeley, CA 94703
Telephone: (510) 289-1626

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

CAROLYN JEWEL, TASH HEPTING, GREGORY HICKS, ERIK KNUTZEN and JOICE WALTON, on behalf of themselves and all others similarly situated,

Plaintiffs,

v.

NATIONAL SECURITY AGENCY, *et al*.,

Defendants.

CASE NO. 08-CV-4373-JSW

PLAINTIFFS' COMBINED REPLY IN SUPPORT OF THEIR MOTION FOR PARTIAL SUMMARY JUDGMENT AND OPPOSITION TO THE GOVERNMENT DEFENDANTS' CROSS-MOTION

Date: December 14, 2012
Time: 9:00 a.m.
Courtroom 11, 19th Floor
The Honorable Jeffrey S. White

TABLE OF CONTENTS

INTRODUCTION 1

ARGUMENT 2

I. Section 1806(f) Displaces The State Secrets Privilege 2

A. The Plain Language and Legislative History of FISA Demonstrate that Section 1806(f) Displaces the State Secrets Privilege 2

1. The Plain Language of Section 1806(f) Applies to Plaintiffs' Claims 3

2. Legislative History Shows that Section 1806(f) Applies to Civil Cases 7

B. Section 1806(f) "Speaks Directly" to the State Secrets Privilege 8

C. The Government's Legislative History Arguments Fail 11

II. Even if Congress Had Not Displaced the State Secrets Privilege by Enacting Section 1806(f), the State Secrets Privilege Would Not Provide Any Basis for Dismissal or Summary Judgment 14

A. The State Secrets Privilege 14

B. Summary Judgment Based On Application Of The *Reynolds* Evidentiary Privilege Is Improper Because It Cannot Be Decided At This Stage Whether Plaintiffs Will Be Able To Prove Their Case Using Non-Privileged Evidence 17

C. The Government's Privilege Assertion Is Overbroad And Unsupported By An Adequate Showing Of Harm 23

D. Even If They Had Not Been Overruled By *General Dynamics*, None Of *Mohamed's* Three "Exceptional Circumstances" Permitting Threshold Dismissal Applies Here 27

1. The Government Has Not Proven That The Privileged Evidence Demonstrates The Existence Of A Valid Defense 28

2. Litigation Using Only Non-Privileged Evidence Will Not Reveal State Secrets 30

III. The Government's Sovereign Immunity Arguments Lack Merit 31

A. Congress Waived Sovereign Immunity For Plaintiffs' Damages Claims 31

B. Sovereign Immunity Does Not Bar Plaintiffs' Equitable Claims 33

1. Plaintiffs' "*Ultra Vires*" Claims Alleging The Government Officer Defendants Lack Authority To Conduct Dragnet Surveillance Are Not Claims Against The United States And Thus Cannot Be Barred By Sovereign Immunity 33

2. Congress Waived Sovereign Immunity For Plaintiffs' Equitable Relief Claims, Including Plaintiffs' APA Claim 38

CONCLUSION 40

TABLE OF AUTHORITIES

Federal Cases

ACLU v. Barr,
952 F.2d 457 (1991) 6

Alderman v. United States,
394 U.S. 165 (1969) 11, 12

Al-Haramain Islamic Found., Inc. v. Bush,
507 F.3d 1190 (9th Cir. 2007) 9, 11, 17

Al-Haramain v. Obama,
690 F.3d 1089 (9th Cir. Aug. 7, 2012) 31, 32

American Elec. Power Co. v. Conn.,
__ U.S. __, 131 S.Ct. 2527 (2011) 9, 10, 11

Aminoil U.S.A., Inc. v. California State Water Resources Control Bd.,
674 F.2d 1227 (9th Cir. 1982) 38

Assiniboine & Sioux Tribes v. Bd. of Oil & Gas,
792 F.2d 782 (9th Cir. 1986) 38

Astoria Fed. Savs. & Loan Ass'n v. Solimino,
501 U.S. 104 (1991) 9

Block v. North Dakota,
461 U.S. 273 (1983) 40

Boumediene v. Bush,
553 U.S. 723 (2008) 1

Bruesewitz v. Wyeth LLC,
__ U.S. __,131 S.Ct. 1068 (2011) 14

Central Reserve Life Ins. Co. v. Struve,
852 F.2d 1158 (9th Cir. 1988) 38

Chamber of Commerce v. Reich,
74 F.3d 1322 (D.C. Cir. 1996) 34, 35, 37

Clift v. United States,
597 F.2d 826 (2d Cir. 1979) 18

Crater Corp. v. Lucent Technologies, Inc.,
423 F.3d 1260 (Fed. Cir. 2005) 18

Custis v. United States,
511 U.S. 485 (1994) 31

Department of Navy v. Egan,
484 U.S. 518 (1988) 9

DTM Research v. AT&T,
245 F.3d 327 (4th Cir. 2001) 18

Dugan v. Rank,
372 U.S. 609 (1963) 37

Duncan v. Walker,
533 U.S. 167 (2001) 5, 32

EEOC v. Peabody Western Coal Co.,
610 F.3d 1070 (9th Cir. 2010) 37

Free Enter. Fund v. Pub. Co. Accounting Oversight Bd.,
130 S.Ct. 3138 (2010) 27

General Dynamics Corp. v. U.S.,
__ U.S. __, 131 S.Ct. 1900 (2011) ..... *passim*

Golinski v. U.S. Office of Personnel Mgmt.,
824 F. Supp. 2d 968 (N.D. Cal. 2012) 16

Gregory v. Ashcroft,
501 U.S. 452 (1991) 10

Halkin v. Helms,
598 F.2d 1 (D.C. Cir. 1978) 18

Halkin v. Helms,
690 F.2d 977 (1982) 23

Hamdi v. Rumsfeld,
542 U.S. 507, 536 (2004) 1

Harmon v. Brucker,
355 U.S. 579 (1958) 35

Hepting v. AT&T Corporation,
439 F. Supp. 2d 974 (N.D. Cal. 2006) 26, 27

In re Evans,
452 F.2d 1239 (D.C. Cir. 1971) 13

In re Sealed Case,
310 F.3d 717 6

In re Sealed Case,
494 F.3d 139 (D.C. Cir. 2007) ..... *passim*

In re United States,
872 F.2d 472 (D.C. Cir. 1989) 18

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

Larson v. Domestic & Foreign Commerce Corp.,
337 U.S. 682 (1949) 34, 35, 36, 37

Maine v. Thiboutot,
448 U.S. 1 (1980) 4

Match-E-Be-Nash-She-Wish Band of Pottawatomi Indians v. Patchak,
__ U.S. __, 132 S.Ct. 2199 (2012) 39, 40

Milwaukee v. Ill.,
451 U.S. 304 (1981) 9, 10

*Mistretta v. United State*s,
488 U.S. 361 (1989) 7

Mohamad v. Palestinian Auth.,
___ U.S. ___; 132 S.Ct. 1702 (2012) 7, 33

Mohamed v. Jeppesen Dataplan, Inc.,
614 F.3d 1070 (9th Cir. 2010) (en banc) ..... *passim*

Monarch Assurance P.L.C. v. United States,
244 F.3d 1356 (Fed. Cir. 2001) 18

Morrison v. Olson,
487 U.S. 654 (1988) 7

Palomar Pomerado Health System v. Belshe,
180 F.3d 1104 (9th Cir. 1999) 38

Pennhurst State School & Hospital v. Halderman,
465 U.S. 89 (1984) 37, 38

Pension Benefit Guaranty Corp. v. LTV Corp.,
496 U.S. 633 (1990) 13

Philadelphia Co. v. Stimson,
223 U.S. 605, 620 (1912) 35

Presbyterian Church (U.S.A.) v. U.S.,
870 F.2d 518 (9th Cir. 1989) 37, 38, 39

Tenet v. Doe,
544 U.S. 1 (2005) 15, 23

Totten v. United States,
92 U.S. 105 (1876) 14, 15, 16

Trudeau v. FTC,
456 F.3d 178 (D.C. Cir. 2006) 38, 39

U.S. v. Nixon,
418 U.S. 683 (1974) 9

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

U.S. v. Texas,
507 U.S. 529 (1993) 10

U.S. v. Vielguth,
502 F.2d 1257 (9th Cir. 1974) 13

U.S. v. Yanagita,
552 F.2d 940 (2d Cir. 1977) 13

Weinberger v. Catholic Action of Hawaii/Peace Ed. Project,
454 U.S. 139 (1981) 15, 16

Williams v. Fanning,
332 U.S. 490 (1947) 37

Statutes

5 U.S.C. § 702 ..... *passim*

5 U.S.C. § 704 38

5 U.S.C. § 706 38

18 U.S.C. § 2510 36

18 U.S.C § 2511 ..... 1, 4, 6, 40

18 U.S.C. § 2520 ..... 31, 33, 36, 40

18 U.S.C. § 2526 ..... 12, 13

18 U.S.C. § 2703 ..... 1, 6

18 U.S.C. § 2707 ..... 31, 33, 36, 40

18 U.S.C. § 2711 36

18 U.S.C. § 2712 ..... *passim*

18 U.S.C. § 3504 ..... 12, 13

29 U.S.C. §§ 621-634 10

42 U.S.C. § 4332 15

50 U.S.C. §§ 1801 5

50 U.S.C. § 1806, *et seq*. ..... *passim*

50 U.S.C. §§ 1809 ..... 1, 6, 39

50 U.S.C. § 1810 ..... 31, 36, 39

50 U.S.C. § 1812 40

50 U.S.C. § 1845 39

Federal Rules

Federal Rule of Evidence 501 8

Federal Rule of Evidence 1006 19

Legislative Materials

Joint Explanatory Statement of the Committee of the Conference, H.R. Conf. Rep. No. 95-1720 (1978), *reprinted in* 1978 U.S.C.C.A.N. 4048 8

Senate Report No. 95-701, *reprinted in* 1978 U.S.C.C.A.N. 3973 ..... 12, 13

USA PATRIOT Act of 2001, Pub L. No. 107-56, 115 Stat. 272 33

Other Authorities

S. Select Comm. to Study Governmental Operations with Respect to Intelligence Activities, *Book II: Intelligence Activities and the Rights of Americans* ("Book II"), S. Rep. No. 94-755 (1976) 2

S. Select Comm. to Study Governmental Operations with Respect to Intelligence Activities, *Book III: Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans* ("Book III") S. Rep. No. 94-755 (1976) 2

INTRODUCTION

The government's attempt to secure threshold dismissal of this case is part of a broader pattern. Since September 11, and now through two Administrations, the Executive has engaged in unprecedented assertions of power without regard to the constitutional and statutory limits of its authority. It has correspondingly sought to exclude the Judiciary from adjudicating whether these exercises of Executive power have stayed within the limits set by the Constitution and by Congress.

The government here seeks to transform the state secrets privilege from a powerful but targeted evidentiary shield into a justiciability sword, preventing the Judiciary from engaging in its constitutional duty. Its goal is to convince this court to close its eyes to a program that impacts every American who uses a phone, email or the Internet.

The Judiciary must recognize the dangers of allowing the Executive to distort narrow exceptions like the state secrets privilege into broad unfettered powers to "turn the Constitution on or off at will." *Boumediene v. Bush,* 553 U.S. 723, 765 (2008). Even in the cases involving war powers, the Supreme Court has confirmed that the "'war power does not remove constitutional limitations safeguarding essential liberties.'" *Hamdi v. Rumsfeld,* 542 U.S. 507, 536 (2004) (quotation omitted). The role of safeguarding those liberties includes the Judiciary: "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." *Id*. at 536.

In fact, Congress has already weighed in, multiple times, on the role of the judiciary in review of the legality of electronic surveillance, creating civil causes of action to remedy illegal electronic surveillance in 18 U.S.C. § 2712, 50 U.S.C. §§ 1809-10, 18 U.S.C § 2511, 18 U.S.C. § 2703 and a procedure in 50 U.S.C. § 1806(f) ("Section 1806(f)") for accommodating national security concerns while ensuring that a court determines the legality of the surveillance. The proper role of the Judiciary, then, is to apply those statutes without altering the balance that Congress struck. That is what plaintiffs seek.

ARGUMENT

I. Section 1806(f) Displaces The State Secrets Privilege

A. The Plain Language and Legislative History of FISA Demonstrate that Section 1806(f) Displaces the State Secrets Privilege

As explained in plaintiffs' opening brief, ("Plainitiffs' Br.," Dkt. #83) the Foreign Intelligence Surveillance Act ("FISA") grew out of the electronic surveillance scandals of the 1960s and 1970s that the Church Committee uncovered. S. Select Comm. to Study Governmental Operations with Respect to Intelligence Activities, *Book II: Intelligence Activities and the Rights of Americans* ("Book II"), S. Rep. No. 94-755 at 12 (1976) (concluding that "surveillance . . . was often conducted by illegal or improper means"). A well-documented part of this scandal was a massive espionage program operated by the NSA, known as SHAMROCK, which is disturbing similar to the NSA's warrantless surveillance programs at issue here. Under it, with the assistance of the international telegraph companies, most international telegrams leaving the United States in the thirty years between 1945 and 1975 were intercepted and copies were provided to the NSA. In the last two or three years of SHAMROCK's existence, about 150,000 telegrams per month were reviewed by NSA analysts. S. Select Comm. to Study Governmental Operations with Respect to Intelligence Activities, *Book III: Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans* ("Book III") S. Rep. No. 94-755 at 765 (1976). As here, most of those illegally surveilled were not prosecuted and the surveillance evidence was never formally used against them by the government.

Against this unseemly backdrop, FISA was enacted to protect ordinary Americans from untargeted dragnet surveillance under the banner of "national security." The civil remedies for illegal surveillance are therefore an essential part of FISA's scheme, and 1806(f) is an essential part of making the civil remedies work.

The government nevertheless asserts that Section 1806(f) displaces the states secrets privilege only where surveillance evidence is used by the government against an aggrieved person. That contention is contradicted both by the statutory text and the legislative history.

1. The Plain Language of Section 1806(f) Applies to Plaintiffs' Claims

As always, the appropriate starting point is the statutory language itself. Section 1806(f)—which was enacted in 1978 as part of the original FISA statute and has not been amended since—begins by describing the three categories of events to which the section applies:

> Whenever a court or other authority
>
> > [i] is notified pursuant to subsection (c) or (d) of this section, or
> >
> > [ii] whenever a motion is made pursuant to subsection (e) of this section, or
> >
> > [iii] whenever *any motion or request* is made by an aggrieved person *pursuant to any other statute or rule* of the United States or any State before any court or other authority of the United States or any state
> >
> > > to discover or obtain applications or orders or other materials relating to electronic surveillance or
> > >
> > > to discover, obtain, or suppress evidence or information obtained or derived from electronic surveillance under this chapter . . . .

Section 1806(f) (indents, line breaks, bracketed numbers and italics added). The first two categories, [i] and [ii], address situations in which the government is intending to use surveillance evidence against a person: the first arises when surveillance evidence is used against a person in a judicial or administrative proceeding (§ 1806(c); § 1806(d)), the second arises when a person moves to suppress surveillance evidence (§ 1806(e)). The government does not dispute that section 1806(f) displaces the state secrets privilege in those two categories. Nor is there any doubt that, whatever the scope of the third category [iii], it too displaces the state secrets privilege for matters within its scope.

This action falls under the third category, which applies when an "aggrieved person," including the plaintiff in an unlawful surveillance civil action, makes "any motion or request," pursuant to "any other statute or rule" including pursuant to the discovery provisions of the Federal Rules, "to discover or obtain applications or orders or other materials relating to [or obtained or derived from] electronic surveillance."

In each of the three categories, the statute provides that the government may assert its interest in state secrets and trigger the Section 1806(f) national security protocol by stating that the disclosure of "the application, order, and such other materials relating to the surveillance" would

harm the national security.

Section 1806(f) then directs that the Court, "*notwithstanding any other law*," "shall" proceed to review the "materials relating to the surveillance "in camera and ex parte" and "determine whether the surveillance of the aggrieved person *was lawfully authorized and conducted*." *Id.* (italics added). The statute also confirms its application to determinations of the legality of the surveillance in its second sentence, authorizing disclosure to the surveilled person, under appropriate security procedures, where "*necessary to assist in the court in making an accurate determination of the legality of the surveillance*." *Id.* (italics added).

Thus, the statute is plain and unambiguous. It applies when "any" motion or request is made under "any other statute or rule." It requires that when a claim of national security harm is made, the Court must still "determine whether the surveillance of the aggrieved person was lawfully authorized and conducted" and can take steps necessary to assist it "in making an accurate determination of the legality of the surveillance." *Id.* Nothing in the statute limits the determination of legality, or the displacement of the state secrets privilege, to only those situations involving suppression or when the government otherwise seeks to use electronic surveillance evidence against a person. To the contrary, the security protocol, the "notwithstanding any law" provision and the requirement to determine legality apply to all three categories of events.

This plain reading also makes sense given FISA's statutory scheme as a whole. Congress has mandated that FISA and the Wiretap Act are the "exclusive means" by which surveillance is conducted. 18 U.S.C. § 2511(f). Congress provided the Section 1806(f) protocol as the practical process by which to ensure the exclusivity of FISA and Wiretap Act processes, and allow a determination of the legality of electronic surveillance, while still allowing the Attorney General and the court to protect national security.

Against this plain language, the government's arguments fail. First, as noted above, Section 1806(f) expressly applies to "any request or motion" made under "any other statute or rule of the United States or any State." There are no limitations in this language. *See, e.g.*, *Maine v. Thiboutot*, 448 U.S. 1, 4 (1980) ("Given that Congress attached no modifiers to the phrase "and laws" [in Section 1983], the plain language of the statute undoubtedly embraces respondents' claim that

petitioners violated the Social Security Act."). And there is certainly no preservation or endorsement of the state secrets privilege, something Congress manifestly knows how to do.

The rule against surplusage also supports this view. A "cardinal principle of statutory construction" is that courts must "give effect, if possible, to every clause and word of a statute." *Duncan v. Walker*, 533 U.S. 167, 174 (2001) (citation and internal quotations omitted). Congress addressed suppression and other situations in which surveillance evidence is used against a person in the statute in the first two clauses. The third clause extends in those Section 1806(f) procedures to "any motion or request" pursuant to "any other statute or rule of the United States." The third category would be superfluous under the government's argument.[1]

Congress reaffirmed that Section 1806(f) applies to civil cases in enacting 18 U.S.C. § 2712(b)(4) in 2001 as part of the PATRIOT Act. Section 2712 is the basis for plaintiffs' claims in Count IX and XII of the Complaint. It provides a cause of action against the United States for violations of the Wiretap Act or the Stored Communications Act ("SCA," referred to as "ECPA" by defendants), Section 2712(b)(4) *expressly requires* the application of Section 1806(f) to plaintiffs' Wiretap Act and SCA claims brought under Section 2712:

> Notwithstanding any other provision of law, the procedures set forth in section 106(f) [50 U.S.C. § 1806(f)] . . . of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. §§ 1801, *et seq*.) shall be the exclusive means by which materials governed by those sections may be reviewed.

This language is clear and unequivocal. Section 1806(f) is the procedure the Court must use in adjudicating plaintiffs' claims against the United States for Wiretap Act and SCA violations "notwithstanding any other provision of law," including the state secrets privilege. Had Congress wanted to impose the state secrets privilege process—as opposed to the Section 1806(f) process—for handling national security information in civil cases against the United States, it would have exempted Wiretap Act and SCA claims from Section 1806(f). By reiterating in 2001 that Section

[1] This same analysis undermines the government's "list" theory, "*noscitur a sociis*." Government Defendants' Notice of Motion and Motion to Dismiss and for Summary Judgment; Opposition to Plaintiffs' Motion for Partial Summary Judgment ("Gov't Br.") at 37 n.28, Dkt. 102. To the extent that Section 1806(f) is a "list" at all, as explained further below, it is a list of procedures for use of the information gathered by electronic surveillance in multiple contexts, not just when the evidence is being used against a person.

1806(f) applies to the *new* causes of action it was creating against the United States, Congress also confirmed that when it enacted Section 1806(f) in 1978 it intended for the statute to apply to civil as well as criminal cases.

The government chides plaintiffs for focusing on the third category. Gov't Br. 36:5-7. Yet the conclusion that Section 1806(f) applies to civil claims stands even when stepping back to review the entirety of 50 U.S.C. § 1806. Section 1806 as a whole provides different kinds of procedures for several different uses of information obtained by electronic surveillance, including uses not against the person surveilled. Section 1806(a) requires minimization procedures for transfer without the consent of the surveilled person; Section 1806(i) requires destruction of unintentionally acquired information; Section 1806(j) provides procedures for when an emergency employment is not followed by an order approving the surveillance, and Section 1806(k) provides requirements for use as part of consultation with law enforcement on national security matters. The government's assertion that Section 1806 as a whole only applies when information is being used against a person is simply not supported by the plain language of the statute.

The government also makes a circular argument—that since it asserts the state secret privilege over "any and all information that would tend to confirm or deny whether plaintiffs in this action have been subject to" the surveillance activities in the Complaint, Section 1806 cannot possibly allow the determination of whether the surveillance was legal. Gov't Br. at 37:9-18. Yet this argument swallows the statute entirely; Section 1806(f) is the process by which, "notwithstanding any other law," the Court makes the determination of whether surveillance was legal under various causes of action: 18 U.S.C. § 2712, 50 U.S.C. § 1809, 18 U.S.C § 2511, 18 U.S.C. § 2703, as well as the Constitution. The government cannot simply sidestep the question of whether the Section 1806(f) process applies instead of the state secrets privilege by asserting the state secrets privilege over whether someone was subject to surveillance.[2]

[2] *ACLU v. Barr,* 952 F.2d 457 (1991), held that Section 1806(f) applies to civil plaintiffs bringing claims of unlawful surveillance. *Id.* at 465, 469-70 ("Congress also anticipated that issues regarding the legality of FISA-authorized surveillance would arise in civil proceedings and . . . it empowered federal district courts to resolve those issues, *ex parte* and *in camera* whenever the Attorney General files an appropriate affidavit under § 1806(f) . . . .").

2. Legislative History Shows that Section 1806(f) Applies to Civil Cases

The language of the statute is plain and unambiguous, so there is no need for resort to legislative history. *Mohamad v. Palestinian Auth.*, ___ U.S. ___; 132 S.Ct. 1702, 1709 (2012).

However, the legislative history only confirms that Section 1806(f) applies to civil cases and not just to situations in which the government is intending to use the electronic surveillance evidence against a person. The U.S. Senate and the House of Representatives in 1978 passed two different FISA bills, each with a different version of the provision that became Section 1806(f), before ultimately reaching agreement in conference on the FISA that was enacted into law. The Senate bill provided a single protocol for determining the legality of electronic surveillance in both criminal and civil cases. The House bill had two separate protocols for determining the legality of electronic surveillance: One House protocol applied to criminal cases where the government sought to use surveillance evidence against an aggrieved person, *i.e.*, the first two categories of the enacted version of Section 1806(f). The other House protocol applied to civil cases in which a determination of the legality of the surveillance was at issue, *i.e.*, the third category of the enacted version of Section 1806(f). The two House protocols had different standards for disclosure to the aggrieved person, among other differences.

The report of the joint House and Senate Committee of Conference for the enacted version of FISA makes clear that Congress had civil suits firmly in mind when it crafted Section 1806(f) and fully intended to extend Section 1806(f) to civil suits in accordance with its plain language:

> The Senate bill provided a single procedure for determining the legality of electronic surveillance in a subsequent in camera and ex parte proceeding …. The Senate bill also provided that, in making this determination, the court should disclose to the aggrieved person materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance.

The decision of the FISA court of review in *In re Sealed Case*, 310 F.3d 717 (For. Intel. Surv. Rev. 2002) (not related to *In re Sealed Case*, 494 F.3d 139 (D.C. Cir. 2007)), is entitled to no weight. Govt. Br. 43. It does not address Section 1806(f)'s use in civil actions; moreover, decisions of the FISA court are advisory opinions without any jurisprudential authority. Although its judges are Article III judges, they are not exercising the Article III power of deciding cases because a warrant or wiretap application not a "Case or Controversy," only a one-sided ex parte presentation. *Mistretta v. United State*s, 488 U.S. 361, 388-90 & n.16 (1989); *Morrison v. Olson*, 487 U.S. 654, 681 n.20 (1988).

> The House amendments provided two separate procedures of determining the legality of electronic surveillance …. In criminal cases, there would be an in camera proceeding; and the court might disclose to the aggrieved person … materials relating to the surveillance if there were a reasonable question as to the legality of the surveillance and if disclosure would promote a more accurate determination of such legality, or if disclosure would not harm the national security. *In civil suits*, there would be an in camera and ex parte proceeding before a court of appeals; and the court would disclose … to the aggrieved person or his attorney materials relating to the surveillance only if necessary to afford due process to the aggrieved person.

Joint Explanatory Statement of the Committee of the Conference, H.R. Conf. Rep. No. 95-1720 at 31-32 (1978)*, reprinted in* 1978 U.S.C.C.A.N. 4048, 4060-61, ("FISA Conf. Comm. Rep.") (italics added).

In the end, Congress adopted a modified version of the Senate protocol, deeming a single protocol sufficient both for criminal cases and for civil cases in which the aggrieved person was seeking a determination of the legality of electronic surveillance:

> The conferees agree that an in camera and ex parte proceeding is appropriate for determining the lawfulness of electronic surveillance *in both criminal and civil cases*. The conferees also agree that the standard for disclosure in the Senate bill adequately protects the rights of the aggrieved person, and that the provision for security measures and protective orders ensures adequate protection of national security interests.

FISA Conf. Comm. Rep. at 32, 1978 U.S.C.C.A.N. at 4061 (italics added). In short, Congress deliberately chose to make Section 1806(f) available not just to those facing the use of electronic surveillance evidence against them, but to civil plaintiffs seeking vindication of constitutional and statutory rights violated by unlawful surveillance.

B. Section 1806(f) "Speaks Directly" to the State Secrets Privilege

The government contends that Section 1806(f) does not "speak directly" to the question of national security evidence and therefore cannot displace the state secrets privilege. Gov't Br. at 29. The government is twice wrong.

First, in Federal Rule of Evidence 501 Congress has set forth the specific legal standard by which displacement should be judged. Rule 501 states that federal evidentiary privileges are displaced whenever a "federal statute" "provides otherwise." *See* Plaintiffs' Br. at 13-14, n.9. Section 1806(f) meets this test because it is a statute that provides for the use of state secrets

evidence "otherwise" than does the state secrets privilege.

Second, as explained in Plaintiffs' Br. at 12-18, Section 1806(f) in any event speaks directly to the question of the admission of national security evidence that the state secrets privilege would otherwise exclude. *See American Elec. Power Co. v. Conn.*, __ U.S. __, 131 S.Ct. 2527, 2537 (2011) (test for whether Congress displaced common law "is simply whether the statute speaks directly to the question at issue" (internal quotation marks and citations omitted); *Milwaukee v. Ill.*, 451 U.S. 304, 315 (1981). And Section 1806(f) applies "notwithstanding any other law" "whenever any motion or request is made by an aggrieved person pursuant to any other statute or rule of the United States . . . to discover or obtain applications or orders or other materials relating to electronic surveillance." "Notwithstanding any other law" encompasses federal common law by its plain terms, showing Congress' express intent to displace the state secrets privilege. Section 1806(f) could not speak more directly than it does to the state secrets privilege.[3]

Although the government argues that "speaks directly" is the governing standard, it also occasionally conflates it with a different standard—the "clear statement" standard. As one of the government's authorities makes clear, however, where federal common-law adjudicatory principles like evidentiary rules are at issue, such a "clear statement" is unnecessary. *Astoria Fed. Savs. & Loan Ass'n v. Solimino*, 501 U.S. 104, 108 (1991) ("[T]he courts may take it as given that Congress has legislated with an expectation that the [common-law] principle will apply except 'when a statutory purpose to the contrary is evident.' . . . This interpretative presumption is not, however, one that entails a requirement of clear statement, to the effect that Congress must state precisely any intention to overcome the presumption's application to a given statutory scheme" (citations omitted). In any event, Section 1806(f) not only "speaks directly," but no clearer statement can be imagined.

---

[3] The state secrets privilege is a common law, not Constitutional, rule. *General Dynamics Corp. v. U.S.*, __ U.S. __, 131 S.Ct. 1900, 1906 (2011); *accord*, *Al-Haramain Islamic Found., Inc. v. Bush*, 507 F.3d 1190, 1196 (9th Cir. 2007). *Department of Navy v. Egan*, 484 U.S. 518, 527 (1988), addresses only the President's Commander-in-Chief powers to refuse to disclose classified information possessed by the Executive Branch to subordinate members of the Executive Branch, not the state secrets privilege. The passing reference to the state secrets privilege in *U.S. v. Nixon*, 418 U.S. 683 (1974), is dicta.

The government also misapplies the "speaks directly" standard. Most of its argument reduces to the claim that Congress failed to utter the words "state secrets." It has never been the rule, even in the cases the government relies upon, that Congress must make a meta-statement explaining its intent to displace federal common law. The question is "*not* whether Congress had affirmatively proscribed the use of federal common law." *Milwaukee*, 451 U.S. at 315 (italics added); *U.S. v. Texas*, 507 U.S. 529, 534 (1993) ("Congress need not 'affirmatively proscribe' the common-law doctrine at issue"); *Am. Elec. Power*, 131 S.Ct. at 2537 ("Legislative displacement of federal common law does not require the same sort of evidence of a clear and manifest congressional purpose demanded for preemption of state law" (internal quotation marks, alteration and citation omitted)). The government's notion that Congress cannot displace the state secrets privilege unless the statute or *Congressional Record* somewhere incants the words "state secrets" in connection with Section 1806(f) is a myth of its own invention.

For instance, in *Gregory v. Ashcroft*, 501 U.S. 452, 460 (1991), the issue was whether the federal Age Discrimination in Employment Act (29 U.S.C. §§ 621-634), applied to state judges. Because state law was being displaced, the clear-statement rule applied. The Court held that "if Congress intends to alter the usual constitutional balance between the States and the Federal Government, it must make its intention to do so unmistakably clear in the language of the statute." *Gregory*, 501 U.S. at 460 (internal quotation marks and citation omitted).

Yet even in *Gregory*, the Court was "not looking for a plain statement that judges are excluded." *Id.* at 467. What mattered was whether "Congress has made it clear that judges are included," which "does not mean that the Act must mention judges explicitly . . . . Rather, it must be plain to anyone reading the Act that it covers judges." *Id*. (citation omitted). The government's argument boils down to asserting that Congress had to mention explicitly either the state secrets privilege or that civil plaintiffs (as "aggrieved persons") are entitled to the procedure of Section 1806(f)—which would be unnecessary even under its "clear statement" standard.

The "speaks directly" inquiry is practical, not formalistic. The statute at issue in *Kasza v. Browner*, for example, comprehensively regulated the operations of garbage dumps. 133 F.3d 1159, 1167-68 (9th Cir. 1998). The statute authorized the president to exempt federal garbage

dumps from regulation if it was in the "paramount interest of the United States," whether or not that interest was related to national security. *Id.* It had nothing to do with the admission or exclusion of evidence or with judicial proceedings.

The Ninth Circuit concluded there was no displacement of the state secrets privilege by making a practical comparison: "[T]he state secrets privilege and [the garbage-dump statute] have different purposes: one is an evidentiary privilege that allows the government to withhold sensitive information within the context of litigation; the other allows the President to exempt a federal facility from compliance with [the garbage dump] regulatory regime." *Id*.

Here, by contrast, the state secrets privilege and Section 1806(f) share a common purpose and overlap completely: both address the evidentiary and litigation consequences that flow from the government's assertion that national security would be harmed by the disclosure, otherwise compelled by the rules of discovery and evidence, of particular items of evidence. *Al-Haramain*, 507 F.3d at 1196; *see Kasza*, 133 F.3d at 1167. Section 1806(f) creates a different adjudicatory procedure for the same evidence. There is "no room for a parallel track." *Am. Elec. Power*, 131 S.Ct. at 2538.

C. The Government's Legislative History Arguments Fail

The government's remaining legislative history arguments seek to recast FISA as so narrow as to be ineffectual. The government's basic argument is that the legislative history shows that Section 1806(f)'s *ex parte*, *in camera* procedures were intended only to address only the use of surveillance evidence in criminal cases, and specifically to address the Supreme Court's decision in *Alderman v. United States*, 394 U.S. 165 (1969), which held that a criminal defendant was entitled to discovery of transcripts of unlawfully intercepted communications to determine if there was any taint. Because the legislative history shows that Section 1806(f) encompasses *Alderman*-type situations, the government claims that Section 1806(f) is limited only to *Alderman*-type situations.

This argument fails. Most important, the government ignores the House and Senate Conference Committee legislative history of the final version of Section 1806(f) set forth above, which is the surest expression of Congress' intent and makes clear that Section 1806(f) applies to civil cases. Instead, the government relies on the legislative history of an earlier version of Section

1806(f) that lacked a crucial provision that plaintiffs rely upon. The Senate committee report the government relies upon, Senate Report No. 95-701, *reprinted in* 1978 U.S.C.C.A.N. 3973, 4027 (Senate Report) was issued on March 14, 1978, before significant changes to the text of what eventually became Section 1806(f). Gov't Br. at 38-42. That version of Section 1806(f), called 18 U.S.C. § 2526(e) in that bill, did not contain in the third category the following language that plaintiffs rely upon: "to discover or obtain applications or orders or other materials relating to electronic surveillance or." This language was added later by the House, after the Senate Report was issued. 124 Cong. Rec. 28427, 28431 at § 106(g) (S. 1566 as reported by the House September 7, 1978). Instead, at the time of the Senate Report the third category was limited to the words "to discover, obtain, or suppress evidence or information obtained or derived from electronic surveillance under this chapter." S. 1566 (March 14, 1978). Because the language that plaintiffs rely upon is absent from the early version of Section 1806(f) that the Senate Report discusses, that report says nothing about what that language means.

Even more specious is the similar *Alderman*-based argument that Congress recognized that "whether to reveal surveillance information is a matter within the Executive's discretion and is a separate distinct consideration from the procedures that would apply under Section 1806(f) should the Government choose to use such evidence." Gov't Br. at 41. The quoted legislative history pertains strictly to the government's ever-present option in criminal cases whether to use evidence or dismiss a prosecution. Thus, the government's argument that the Senate Report can limit the meaning of the critical language in Section 1806(f) simply fails.

The government's argument with regard to 18 U.S.C. § 3504 actually supports plaintiffs. That statute demonstrates that an "aggrieved person" need not prove that he or she had been subjected to unlawful surveillance; she need only state a colorable basis for so believing. As the government notes, the Senate Report stated that motions made by an "aggrieved person" include motions under 18 U.S.C. § 3504 ("Section 3504"). Gov't Br. at 40; S. Rep. No. 95-701 at 62-63, 1978 U.S.C.C.A.N. at 4031-4032 ("This procedure applies, for example, whenever an individual makes a motion … pursuant to … 18 U.S.C. § 3504…."). The Senate Report did so because the early version of Section 1806(f) that it was discussing made explicit reference to Section 3504, a

reference that was deleted from the final version: "whenever any motion is made by an aggrieved person pursuant to Section 3504 of this title or any other statute or rule." S. 1566 (March 14, 1978).

Section 3504, enacted in 1970, permits a "party aggrieved" who claims that evidence is inadmissible because it is the fruit of illegal surveillance to require the government to "affirm or deny the occurrence of the alleged unlawful act of surveillance." When FISA was enacted in 1978, the courts had established that a party was "aggrieved" and entitled to discovery from the government under Section 3504 so long as the party could state a colorable basis for believing he or she had been subjected to electronic surveillance. *U.S. v. Vielguth*, 502 F.2d 1257, 1258 (9th Cir. 1974) ("the government's obligation to affirm or deny the occurrence of electronic surveillance under Section 3504(a)(1) 'is triggered . . . by the mere assertion that unlawful wiretapping has been used against a party.' "); *In re Evans*, 452 F.2d 1239, 1247 (D.C. Cir. 1971) (same); *U.S. v. Yanagita*, 552 F.2d 940, 943 (2d Cir. 1977) (surveillance allegations that have a "'colorable' basis … function to trigger the government's obligation to respond under [§] 3504"). Because Section 3504 motions are within the scope of Section 1806(f), persons with a colorable basis for alleging they have been surveilled (a standard that plaintiffs easily meet) are "aggrieved persons" for purposes of Section 1806(f).

Finally, even if the government's legislative history had any relevance here, it is clear that the Senate Report's comments regarding Section 1806(f)'s application to criminal prosecutions were meant to be exemplary, not exclusive. *Pension Benefit Guaranty Corp. v. LTV Corp*., 496 U.S. 633, 649 (1990) ("The language of a statute . . . is not to be regarded as modified by examples set forth in the legislative history."). The report explains that the prescribed procedure "applies, for example," in the specified situations. S. Rep. No. 95-701, at 63 (1978). Indeed, the report explains that Section 1806(f) applies broadly whatever the nature of the underlying proceeding:

> The committee wishes to make very clear that the procedures set out in [section 1806(f) now, 18 U.S.C. 2526(c) in the version before the Committee] apply whatever the underlying rule or statute referred to in the motion. This is necessary to prevent the carefully drawn procedures in subsection [f] from being bypassed by the inventive litigant using a new statute, rule or judicial construction.

Ibid. Section 1806(f) was to be exclusive in *all* cases, not just criminal cases. The government is

the "inventive litigant" here.[4]

II. Even if Congress Had Not Displaced the State Secrets Privilege by Enacting Section 1806(f), the State Secrets Privilege Would Not Provide Any Basis for Dismissal or Summary Judgment

A. The State Secrets Privilege

The state secrets privilege would not provide a ground for dismissal or summary judgment even if Congress had not displaced it with Section 1806(f). The state secrets privilege is "a Government privilege against court-ordered disclosure of state and military secrets." *Gen. Dynamics Corp. v. United States*, __ U.S. __, 131 S.Ct. 1900, 1905 (2011). It may be invoked only by the government. *U.S. v. Reynolds*, 345 U.S. 1, 10 (1953). As the Supreme Court explained in *Reynolds*, it is the government's burden to show "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." *Reynolds*, 345 U.S. at 10. The government has not met that burden in this motion.

Like other privileges, the state secrets privilege protects from disclosure evidence possessed by the privilege-holder—it does not bar litigation of the claim to which the evidence relates or the use of other evidence outside the control of the privilege-holder. It is an "evidentiary rule[]: The privileged information is excluded and the trial goes on without it." *Gen. Dynamics*, 131 S.Ct. at 1906. If after full discovery of all nonprivileged evidence, the plaintiff is unable to prove its case, the plaintiff loses, just as happens whenever a plaintiff is unable to carry its burden of proof. *Kasza*, 133 F.3d at 1166.

In addition to the *Reynolds* evidentiary privilege, state secrets play a separate and distinct role in government contract cases, as the Supreme Court explained in *General Dynamics*. Beginning with *Totten v. United States*, 92 U.S. 105 (1876), an attempt to enforce a spy's Civil

[4] Defendants' desperation shows when they argue that a stray comment in a 2007 committee report for the FISA Amendments Act, which notes the government had (unsuccessfully) sought dismissal of the telecommunications carriers lawsuits on state secrets grounds, says something about what Section 1806(f) means. Gov't Br. at 42. A 2007 committee report's views about ongoing litigation are, of course, irrelevant to determining what Congress intended in 1978 when it enacted Section 1806(f). The legislative history of subsequent legislation cannot alter the meaning of an earlier statute. *Bruesewitz v. Wyeth LLC*, __ U.S. __,131 S.Ct. 1068, 1082 (2011). Moreover, if Congress in 2008, knowing that Section 1806(f) had been invoked in *Hepting*, had wanted to end Section 1806(f)'s application to civil plaintiffs, it could have easily amended Section 1806(f) to do so. Its decision not to do so suggests it was untroubled by Section 1806(f)'s application to civil plaintiffs.

War contract, the Supreme Court has held that government contracts are unenforceable if proving their claims or defenses would require secret evidence. *Gen. Dynamics*, 131 S.Ct. at 1906. In such contract cases, public policy "prohibit[s] suits against the Government based on covert espionage agreements." *Tenet v. Doe*, 544 U.S. 1, 3 (2005). *Tenet* was another case brought by spies whose claims all arose out an alleged espionage agreement. *Gen. Dynamics*, 131 S.Ct. at 1906 (*Totten* and *Tenet* are "two cases dealing with alleged contracts to spy").

This case is not a government contracting case. Many lower courts, however, including the Ninth Circuit, had extended the *Totten* bar to non-contract cases not seeking to enforce duties arising from a voluntary relationship between the plaintiff and the government. *Mohamed v. Jeppesen Dataplan, Inc.*, 614 F.3d 1070, 1082 (9th Cir. 2010) (en banc). But the Supreme Court in *General Dynamics* made clear that this was error, holding that the source of its authority for ordering threshold dismissal, rather than simply the exclusion of evidence, in the *Totten-Tenet* line of cases is "our common-law authority to fashion contractual remedies in Government-contracting disputes." *Gen. Dynamics*, 131 S.Ct. at 1906. Refusing to enforce government contracts in those circumstances "captures what the *ex ante* expectations of the parties were or reasonably ought to have been. . . . Both parties . . . must have assumed the risk that state secrets would prevent the adjudication of [their] claims . . . ." *Id.* at 1909. This reasoning has no application to cases not based on a contract between the plaintiff and the government. In non-contract cases, it is the *Reynolds* evidentiary privilege that applies, a product of the Supreme Court's "power to determine the procedural rules of evidence." *Gen. Dynamics*, 131 S.Ct. at 1906.[5]

---

[5] The government resists this conclusion, arguing that *Tenet* held that the *Totten* bar applies outside of cases based on a contract or other voluntary relationship between the plaintiff and the government. Gov't Br. at n.9. The government's argument lacks merit; it is inconsistent not only with *General Dynamic's* description of *Tenet* but with *Tenet* itself: "*Totten's* core concern . . . [is] preventing the existence of the plaintiff's relationship with the Government from being revealed," *Tenet*, 544 U.S. at 10; in *Totten*, "we thought it entirely incompatible with the nature of such a contract that a former spy could bring suit to enforce it," *id*. at 7-8; "the categorical *Totten* bar" applies "in the distinct class of cases that depend upon clandestine spy relationships," *id*. at 9-10. Moreover, given that *Tenet* was a government contract case, any suggestion by it that the *Totten* bar applied outside of contract cases would have been dicta.
The government's reliance on *Weinberger v. Catholic Action of Hawaii/Peace Ed. Project*, 454 U.S. 139 (1981), is similarly misplaced. Gov't Br. at 15. The government did not invoke the state secrets privilege in that case. Instead, the case was about statutory interpretation, holding that in the

Given that the authority for the *Totten* bar is the common-law power to fashion contractual remedies and that the reasoning supporting it rests on contractual expectations, the *Totten* bar has no application to non-contract cases like this one. Before *General Dynamics*, the Ninth Circuit in *Mohamed* had identified three "exceptional circumstances" (614 F.3d at 1077) in which the state secrets doctrine permits threshold dismissal of a lawsuit. As applied to non-contract cases like this one, none of the three exceptions survives *General Dynamics*.

The first exception is where the "very subject matter" of the lawsuit is a state secret. *Mohamed*, 614 F.3d at 1077-78. This is the Ninth Circuit's generalization of the *Totten* bar to non-contract cases, which, as explained above, was effectively overruled in *General Dynamics*. *Gen. Dynamics*, 131 S.Ct at 1906.

The second exception is where the excluded evidence makes it impossible for the defendant to prove up a *valid* defense. *Mohamed*, 614 F.3d at 1083. The third of these "rare circumstances" permitting dismissal is where litigating the action using only non-privileged evidence inevitably "would create an unjustifiable risk of revealing state secrets." *Mohamed*, 614 F.3d at 1083, 1088-89. The Ninth Circuit held in *Mohamed* that dismissals under the valid-defense or the unjustifiable-risk exceptions were authorized by *Reynolds*. *Mohamed*, 614 F.3d at 1083. *General Dynamics*, however, held that *Reynolds* was an evidentiary rule whose only consequence was to exclude evidence, that it was *Totten*, not *Reynolds*, that authorized such dismissals, and that *Totten* dismissals were a consequence of the common law of contracts. *Gen. Dynamics*, 131 S.Ct. at 1906, 1907, 1909, 1910. "*Reynolds* was about the admission of evidence. It decided a purely evidentiary dispute by applying evidentiary rules." *Id*. at 1906. *General Dynamics* thus has effectively overruled *Mohamed*'s conclusion that *Reynolds* creates these two exceptions and that they can be applied to dismiss non-contract cases at the threshold. *See Golinski v. U.S. Office of Personnel Mgmt.*, 824 F. Supp. 2d 968, 983-85 (N.D. Cal. 2012).

National Environmental Policy Act, 42 U.S.C. § 4332(2)(C), Congress had expressly exempted from public disclosure any Environmental Impact Statement involving classified information. *Weinberger*, 454 U.S. at 142-45. Here, of course, Congress has created both the causes of action and the process by which a court must determine if the surveillance is legal.

B. Summary Judgment Based On Application Of The *Reynolds* Evidentiary Privilege Is Improper Because It Cannot Be Decided At This Stage Whether Plaintiffs Will Be Able To Prove Their Case Using Non-Privileged Evidence

Even if these three threshold-dismissal exceptions applied to non-contract cases, neither they nor the *Reynolds* evidentiary privilege would provide a basis for dismissal here.

The government contends that without privileged evidence plaintiffs will not be able to prove their claims. This assertion is incorrect, but in any event it is a determination that cannot be made at this threshold, but only after discovery and further proceedings. Application of the *Reynolds* evidentiary privilege can result in dismissal or summary judgment only if, after full discovery and application of the privilege to specific items of evidence, plaintiffs are unable to present a prima facie case. Here the question cannot yet be answered, and judgment for the government is improper, because the universe of non-privileged evidence that plaintiffs may rely on is not yet known: plaintiffs have not yet propounded any discovery, either to the government or to third parties, and the government has not yet asserted the privilege in response to specific evidentiary requests. To that end, plaintiffs have filed a 56(d) declaration with this opposition as well as a large amount of nonsecret evidence and a Summary of Voluminous Evidence that provides an overview of the breadth of information already available.

A court is in no position to determine whether a plaintiff can prove up a prima facie case until after discovery has proceeded, the government has asserted the state secrets privilege with respect to specific items of evidence, the court has " 'critically . . . examine[d]' " the privilege assertion as to each item of evidence, and, in instances in which it has sustained the privilege, has "'disentangled'" privileged information from nonprivileged information. *Mohamed*, 614 F.3d at 1082. "The plaintiff's case then *goes forward* based on evidence not covered by the privilege." *Kasza*, 133 F.3d at 1166 (italics added). "The privileged information is excluded and the trial goes on without it" (*General Dynamics*, 131 S.Ct. at 1906), " 'with no consequences save those resulting from the loss of evidence.' " *Mohamed*, 614 F.3d at 1082; *see also Al-Haramain*, 507 F.3d at 1204 ("[t]he effect of the government's successful invocation of privilege 'is simply that the evidence is unavailable, as though a witness had died, and the case will proceed accordingly'").

As in any case in which evidence is excluded because of a privilege, dismissal is possible if

after full discovery the plaintiff is unable to prove its case using nonprivileged evidence. "If, *after further proceedings*, the plaintiff cannot prove the *prima facie* elements of her claim with nonprivileged evidence, then the court may dismiss her claim as it would with any plaintiff who cannot prove her case." *Kasza*, 133 F.3d at 1166 (emphasis added); *accord*, *Mohamed*, 614 F.3d at 1083. None of these necessary steps has yet occurred in this case.

Accordingly, this Court should decline to decide at this time whether plaintiffs will be able to prove their case using nonprivileged evidence. That course of proceedings is what happened in *Kasza*, which was not dismissed until after discovery had gone forward. It is what happened in *Reynolds*, where after excluding the privileged evidence the Supreme Court remanded for further proceedings to give the plaintiffs the opportunity "to adduce the essential facts as to causation without resort to material touching upon military secrets." 345 U.S. at 11. It is what happens in state secrets cases generally. *See*, *e.g.*, *In re Sealed Case*, 494 F.3d at 153 (D.C. Cir. 2007) (remanding for further proceedings); *Crater Corp. v. Lucent Technologies, Inc.*, 423 F.3d 1260, 1268-69 (Fed. Cir. 2005) (reversing dismissal because record was not sufficiently developed to determine whether claims could proceed without the excluded state secrets evidence); *DTM Research v. AT&T*, 245 F.3d 327, 334 (4th Cir. 2001) ("the plaintiff's case should be allowed to proceed"); *Monarch Assurance P.L.C. v. United States*, 244 F.3d 1356, 1364 (Fed. Cir. 2001) (holding dismissal was "premature" because plaintiff should be "give[n] a fair amount of leeway" "in building their case from non-government sources"); *In re United States*, 872 F.2d 472, 478 (D.C. Cir. 1989) ("an item-by-item determination of privilege will amply accommodate the Government's concerns"); *Clift v. United States*, 597 F.2d 826, 827-30 (2d Cir. 1979) (reversing dismissal because plaintiff "has not conceded that without the requested documents he would be unable to proceed, however difficult it might be to do so"); *Halkin v. Helms*, 598 F.2d 1, 11 (D.C. Cir. 1978) (case remanded for further proceedings to determine whether the plaintiffs could prove some of their claims without resort to state secrets evidence).

Even if it were proper to determine the question on this record, the government's argument that it will be impossible for plaintiffs to present a prima facie case is conclusory and abstract, divorced from any reference to specific items of evidence. DNI Clapper's privilege assertion is

similarly inadequate for this purpose because it does not address specific discovery requests or specific items of evidence. It claims the privilege over broad categories of "information," not over specific items of evidence within the government's control. Clapper Decl. ¶¶ 11-26; *see Mohamed*, 614 F.3d at 1080 ("The claim also must be presented in sufficient detail for the court to make an independent determination of the validity of the claim of privilege and the scope of the evidence subject to the privilege."). In addition, the government ignores the evidence proffered by plaintiffs demonstrating the existence and operation of the government's dragnet, untargeted surveillance program. Pls.' Fed. R. of Evid. 1006 Summ. of Voluminous Evid. at 6-14, 19-24.[6]

The government makes two contentions in support of its argument that plaintiffs cannot present a *prima facie* case. First, it contends that plaintiffs will be unable to prove the injury-in-fact component of their standing. Gov't Br. at 25. This contention fails. Plaintiffs have not just alleged injury in fact but have set forth an extensive factual record demonstrating interception and acquisition of their communications and communications records. As explained at length in plaintiffs' memorandum in support of their motion for partial summary judgment, this record includes the Klein and Marcus declarations and associated AT&T documents (Dkt #85, 89) establishing that AT&T has installed special fiber-optic "splitters" that make a copy of every communication passing over the links between AT&T's Internet network and the Internet networks of other telecommunications carriers and divert the copy to a secret room controlled by the NSA filled with powerful computers. Klein Decl ¶¶ 24-34 (Dkt. #85); Marcus Decl.¶¶ 56-72 (Dkt. # 89); SOE at 6-9. The declarations of Messrs. Binney, Wiebe and Drake further demonstrate injury in fact by confirming that the NSA is conducting wholesale, untargeted collection of communications and communications records. Binney Decl. ¶¶ 7-17 (Dkt #88); Wiebe Decl. ¶¶ 6-14 (Dkt #86); Drake Decl. ¶¶ 8-10 (Dkt #87).

In addition plaintiffs file herewith voluminous evidence demonstrating injury-in-fact, including government admissions that demonstrate the untargeted collection of the

[6] The evidence is summarized in Plaintiffs' Summary of Voluminous Evidence under Federal Rule of Evidence 1006, filed herewith with citations to the evidence itself, which is attached as exhibits to the Declaration of Kurt Opsahl, also filed herewith. Collectively these will be referred to as "SOE."

communications of Americans.[7] SOE at 6-14, 19-24. For instance, James Baker, head of the Justice Department's Office of Intelligence Policy and Review (who is read in to the Program), agreed that the following description was a "fair assessment" of the Program's operation:

> So what you're saying is that with modern communications, it's almost inevitable that you're going to collect, *in the sense of initially acquire*, communications of innocent people, of Americans who are not suspected of terrorism[.]

SOE at 10-11. Similarly, John Yoo, a Department of Justice official assigned to oversee the Program confirmed in a television interview that, in his view the government "needs to have at least access to the flow [of communications]; . . . In order to get Internet messages, you have to be able to dip into the flow of communications, because Internet communications are broken up ... I don't think it's inherently always wrong for communications providers to give the government access to the networks."). SOE at 11**.** These are only two admissions of many. Admissions also abound in congressional testimony, *see, e.g.*, SOE at 15 (McConnell testimony admitting that U.S. person information is intercepted and stored in the government's databases); SOE at 48 (McConnell testimony admitting that the government does not consider "metadata" content). A critical report by the Inspectors General of the Justice Department, Defense Department, the Central Intelligence Agency, the National Security Agency, and the Office of the Director of National Intelligence contains further admissions. SOE at 1, 34-38, 44-46. In addition, members of Congress have been quoted in news media and elsewhere confirming key elements of the surveillance. *See, e.g.*, SOE at 19-23. For instance, then-Senator Bob Graham, who chaired the Intelligence Committee at the time, stated that briefers told him that "Bush had authorized . . . the NSA to intercept conversations that . . . went through a transit facility inside the United States." SOE at 10. And injury-in-fact is confirmed by the media coverage describing the surveillance in

[7] Note that the Administration officials have engaged in significant misdirection about their activities due to careful wording and hidden, cramped definitions to terms like "collection" "surveillance," conversation" and "communications," SOE at 46-49, some of which they were later forced to admit. *Id*. Here they continue to do so with their carefully crafted assertions and denials. *Compare* Fleisch Decl. ¶ 3 ("Plaintiffs allege that the presidentially-authorized activities at issue in this litigation went beyond the "Terrorist Surveillance Program"), *with* SOE at 44-46 (noting government confirmation that the Program included "other intelligence activities," beyond the narrowly defined "TSP").

detail, including books, newspapers, radio and television news and new magazines. *See generally* SOE at 2-25.

The government also errs in asserting that "plaintiffs cannot adduce proof that the content of their communications or their communications records have been collected by the Government" because "information concerning whether plaintiffs have been surveilled by the NSA is specifically protected by the Government's state secrets assertion." Gov't Br. at 25-26. The state secrets privilege does not cover all information concerning whether plaintiffs have been surveilled; the privilege assertion extends at most only to certain nonpublic evidence possessed or controlled by the government and does not extend to independent evidence possessed by those, like former AT&T engineer Mark Klein, who owe no duty to the government to keep it secret. *Mohamed*, 614 F.3d at 1090 (a "claim of privilege does not extend to public documents"). Indeed, the government has conceded not just that the Klein and Marcus declarations and the associated AT&T documents are not subject to the state secrets privilege but also that none of the subjects addressed in those documents are state secrets. Plaintiffs' Request for Judicial Notice filed herewith, Ex. A.

This is just one example of how the government's state secrets analysis conflates the "disclosure"—by anyone—of "information" on various topics with the exclusion of specific privileged *government* evidence relating to those topics. The state secrets privilege, however, is limited to protecting secret evidence possessed by the government; it does not bar litigation of an issue using nongovernment evidence, or nonsecret government evidence and admissions, just because the government also possesses privileged evidence relating the issue.

In a similar vein, the government also mischaracterizes plaintiffs' complaint as "quite clearly seek[ing] disclosure of whether or to what extent the Government may have utilized certain intelligence sources and methods" and as "seek[ing] disclosure of whether any of the alleged activities . . . are ongoing." Gov't Br. at 14; *see also id*. at 24 ("the very purpose of the litigation is to obtain the disclosure of NSA sources and methods"). Plaintiffs' complaint seeks disclosure of nothing. Plaintiffs will propound discovery requests seeking information from the government and others relating to their claims, but their claims are not disclosure claims and of course the Section 1806(f) procedures allow the government to trigger *ex parte*, *in camera* review so that, for the

government's own appropriately secret evidence, no disclosure occurs.

A related unspoken assumption of the government's position is that no matter how much nonprivileged evidence plaintiffs muster, plaintiffs cannot prove the merits of their claims without an admission of liability from the government. But " '[a]s in any lawsuit, the plaintiff may prove his case by direct or circumstantial evidence.' " *In re Sealed Case*, 494 F.3d at 147. The evidence plaintiffs already possess demonstrates the feasibility of proving their claims without additional admissions by the government.

Importantly, to prove their claims plaintiffs need not, and do not seek to prove what the government did with the communications and communications records they intercepted and acquired, including whatever analysis or targeting the government may have subsequently applied to that mass of information. Nor are the contents of the intercepted communications and records relevant. In particular, because the statutory and constitutional violations plaintiffs allege are complete upon the interception and acquisition of plaintiffs' own communications and records as part of a program of warrantless, untargeted, mass surveillance, plaintiffs' claims do not require any "disclosure of whether specific individuals were targets of alleged NSA activities." Gov't Br. at 21. Plaintiffs allege they were unlawfully subjected to untargeted surveillance and need not prove that anyone was targeted. Nor is it correct, as the government and DNI Clapper suggest, that proving plaintiffs were subjected to mass, untargeted surveillance would reveal the identities of anyone who was targeted for surveillance. As discussed further below, their error lies in erroneously equating the question of whether a person was "subject to" surveillance with the altogether different question of whether a person was a "target of" surveillance. *See*, *e.g.*, Gov't Br. at 21; Clapper Decl. ¶ 22; Fleisch Decl. ¶¶ 16-17.

Thus, this lawsuit cannot be dismissed on the unsupported premise that plaintiffs will in the future be unable to prove their case with nonprivileged evidence. Instead, the case must proceed forward, " 'with no consequences save those resulting from the loss of evidence.' " *Mohamed*, 614 F.3d at 1082.

C. The Government's Privilege Assertion Is Overbroad And Unsupported By An Adequate Showing Of Harm

Even if it were not the case that Section 1806(f) displaces the state secrets privilege, the government's assertion of the state secrets privilege would provide no basis for dismissing this action or granting summary judgment. That is not all, however. The government's privilege assertion is overbroad and unsupported by an adequate showing of harm.

Reynolds "set out a balancing approach for courts to apply in resolving Government claims of privilege." *Tenet*, 544 U.S. at 9. A state secrets privilege assertion is sustainable only if it is supported by a credible showing that there is a "'reasonable danger'" that disclosure of any of the evidence within the scope of the privilege assertion would harm national security. *Reynolds*, 345 U.S. at 10; *accord*, *Kasza*, 133 F.3d at 1170 (evaluating whether disclosure "would reasonably endanger national security"); Gov't Br. at 17.

The "critical feature of the inquiry" "is whether the *showing* of harm that might reasonably be seen to flow from disclosure is adequate in a given case to trigger the absolute right to withhold the information sought." *Halkin v. Helms*, 690 F.2d 977, 990 (1982) (italics original). The scope of the privilege and the asserted harm must be coextensive: To adequately support the claim of privilege, the asserted harm must be reasonably likely to occur if any of the evidence within the scope of the privilege is disclosed; otherwise, the privilege assertion is overbroad. Thus, the broader and less specific the identification of the evidence subject to the claim of privilege, the greater the showing necessary to demonstrate that disclosure of *any* of the evidence falling within the scope of the assertion is reasonably likely to harm national security. A privilege assertion can also fail if evidence within the scope of the assertion is not actually secret and has already been disclosed by the government.

Moreover, the court must review the government's assertion of an overriding national security interest " 'with a very careful, indeed a skeptical, eye, and not to accept at face value the government's claim or justification of privilege.' " *Mohamed*, 614 F.3d at 1082.

The Clapper and Fleisch declarations discuss the "TSP" almost exclusively. The TSP, by definition, is a label given to portions of the broader program directed to communications to which a foreign person associated with terrorism communicates from foreign soil to a person within the

United States. This case is not about the TSP. This case is about the domestic seizure and storage of the electronic communications, including purely domestic communications, of persons within the United States, as well as the acquisition of the communications records of those persons. As a consequence, the statements within the Clapper and Fleisch declarations to the effect that foreign terrorist groups on foreign soil remain intent on attacking U.S. interests are completely beside the point. *See* Clapper Decl. ¶¶ 12-21; Fleisch Decl. ¶ 11.

DNI Clapper asserts the privilege first over "information that would reveal whether particular individuals, including the named plaintiffs . . . , have been *subject to* alleged NSA intelligence activities," *i.e.*, untargeted dragnet surveillance, as this is the only NSA intelligence activity plaintiffs allege they have been subject to. Clapper Decl. ¶ 22 (italics added). The harm he asserts is that revealing whether plaintiffs have been "subject to" *untargeted* surveillance would reveal which individuals were or were not "*targets of*" surveillance. *Id*. His claim of harm lacks merit because it is a non sequitur. He erroneously equates those who are "subject to" untargeted surveillance with "targets of" surveillance by silently substituting the latter for the former from one sentence to the next. *Id.* Plaintiffs were *subjected to* surveillance but were not *targets of* surveillance because the surveillance to which they were subjected was untargeted. Complaint ¶¶ 2, 3, 7, 9, 10, 70, 74, 77-79, 82, 90, 93-95, 110, 120, 129, 138. Proving plaintiffs were unlawfully surveilled by untargeted surveillance will not involve proving that any person was (or was not) a target of surveillance.

DNI Clapper makes an omnibus circular privilege assertion over "any other facts concerning NSA intelligence activities, sources, or methods that may relate to or be necessary to litigate the plaintiffs' claims." Clapper Decl. ¶ 23. On its face, this assertion is meaninglessly overbroad: it has no fixed meaning because its scope is not defined by any objective criteria but simply reflexively as whatever information plaintiffs need for litigation. This simplistic "if plaintiffs need it, then it must be secret" approach is facially inadequate to define what evidence the privilege is being asserted over, much less to demonstrate that everything within this broad and amorphous description is secret and that disclosure of any of it would harm national security. *See Mohamed*, 614 F.3d at 1080 ("The claim also must be presented in sufficient detail for the court to

make an independent determination of the validity of the claim of privilege and the scope of the evidence subject to the privilege."). And, of course, much of what falls within this description is not secret at all. A wealth of evidence, from statements made by government officials to third-party witnesses, all provide important information to assess the legality of the Program. *See generally* SOE**.**

Within this overbroad privilege assertion, DNI Clapper identifies three narrower subjects. The first is "facts concerning the operation of the now-inoperative Terrorist Surveillance Program." Clapper Decl. ¶¶ 23, 24. Many of the facts describing the broader President's Program have been publicly disclosed by government officials. *See*, *e.g.***,** SOE 9-11, 11-13, 14-16. In any event, as noted above, the activities labeled the "TSP" consisted of targeted surveillance activities; plaintiffs were subjected to (and their claims are limited to) untargeted surveillance. Clapper Decl. ¶ 24 (TSP "directed at" al-Qaeda members). Plaintiffs need not and do not intend to prove any secret "facts concerning the operation of the now-inoperative Terrorist Surveillance Program." This privilege assertion is irrelevant.

The second subject is "any facts needed to demonstrate . . . that the NSA does not otherwise conduct a dragnet of content surveillance as the plaintiffs allege." Clapper Decl. ¶¶ 23, 24. Unlike DNI Clapper's other privilege assertions, which cover information relating to either the existence or nonexistence of a particular fact (*id*. at ¶¶ 11(B) ("Information that may tend to confirm or deny"), 11(C)(ii) ("Information concerning whether or not"), 11(C)(iii) ("Information that may tend to confirm or deny")), this one deliberately is limited to facts on only one side of the coin—only facts demonstrating that the NSA does not conduct dragnet surveillance. To the extent wishes to use this assertion as the basis for invoking the valid-defense exception, it has failed to follow the proper procedure for doing so, as explained below. To the extent the government makes this assertion for any other purpose, it is irrelevant; unsurprisingly, plaintiffs do not seek any evidence showing that the NSA does *not* conduct dragnet surveillance.

The third subject is "information concerning whether or not the NSA obtains transactional communications records from telecommunications companies such as AT&T." Clapper Decl. ¶¶ 23, 25. The asserted harm would come simply from "confirmation or denial" of this fact.

Clapper Decl. ¶ 25. As noted above, plaintiffs do not require a government admission to prove their case. Regardless, however, this fact has been confirmed by numerous members of Congress "read in" to the secrets of these intelligence activities. SOE at 19-25. For instance, Senator Kit Bond confirmed: "The president's program uses information collected from phone companies. The phone companies keep their records. They have a record. And it shows what telephone number called what other telephone number." SOE 20. And then-Senate Majority leader William Frist also confirmed that he was one of the people briefed on a program by which the National Security Agency has been secretly collecting the phone call records of tens of millions of Americans using data provided by AT&T, Verizon and BellSouth. SOE at 20. In total, nine members of Congress, each fully briefed on "the entire scope of NSA surveillance," acknowledged the call records program publicly and on-the-record. SOE at 23. Accordingly, because this fact has already been publicly confirmed by knowledgeable government officials, in addition to a tremendous number of media sources, no additional harm can come from using that same fact in litigation and the privilege assertion is moot.

DNI Clapper next asserts the privilege over "information that may tend to confirm or deny whether or not AT&T . . . or . . . any other particular telecommunications provider has assisted the NSA with alleged intelligence activities." Clapper Decl. ¶ 26. As the court has already found, this information is not a secret because "public disclosures by the government and AT&T indicate that AT&T is assisting the government to implement some kind of surveillance program." *Hepting v. AT&T Corporation*, 439 F. Supp. 2d 974, 994 (N.D. Cal. 2006). Former DNI McConnell, in fact, confirmed that the telecommunications companies being sued in the *In re NSA Telecommunications* multidistrict litigation, which included AT&T, "had assisted us." SOE at 25-26. Other evidence exists as well. SOE 26-28. This privilege assertion thus fails.

DNI Clapper asserts the privilege over "information concerning the specific nature of the terrorist threat posed by al-Qa'ida and its affiliates and other threats to the United States." Clapper Decl. ¶ 11(A). The information covered by this privilege assertion is irrelevant to plaintiffs' claims, which are limited to untargeted surveillance and do not require proof of who was targeted for surveillance, why they were targeted, or what their connection to al-Qaeda or other organizations

was. Nor do plaintiffs' claims require disclosure of the contents of any intercepted communications. Thus, any privilege over specific information about the al-Qaeda threat or other threats is not an obstacle to litigation of plaintiffs' claims.

Finally, the privilege assertion here is procedurally defective. "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." *Reynolds*, 345 U.S. at 7-8. Here, that department head is the Secretary of Defense, not the Director of National Intelligence. Even assuming that the Office of Director of National Intelligence is a "department" for purposes of *Reynolds*, *see Free Enter. Fund v. Pub. Co. Accounting Oversight Bd.*, 130 S.Ct. 3138, 3162 (2010) (for purposes of the Appointments Clause, a "'department'" is a "free-standing, self-contained entity in the Executive Branch"), it is not the "department which has control over the matter" because it does not command the NSA, a unit of the Department of Defense. Fleisch Decl. ¶ 5. The Fleisch declaration is also insufficient, since the NSA is not a "free-standing, self-contained entity in the Executive Branch," and thus a declaration by its Director, Deputy Director, or any other NSA officer is inadequate to invoke the state secrets privilege.

D. Even If They Had Not Been Overruled By *General Dynamics*, None Of *Mohamed*'s Three "Exceptional Circumstances" Permitting Threshold Dismissal Applies Here

As the Supreme Court emphasized in *General Dynamics*, a threshold dismissal on state secrets grounds "is the option of last resort, available in a very narrow set of circumstances." 131 S.Ct. at 1910. Even if *General Dynamics* had not effectively overruled *Mohamed* and the three contract-based threshold dismissal exceptions still applied in non-contract lawsuits, none of them would provide a basis for dismissal here.

The government does not contend that the "very subject matter" of plaintiffs' lawsuit is a state secret, and so the first *Mohamed* exception does not apply. *Mohamed*, 614 F.3d at 1077-78. The government is wise not to make this argument. This Court in *Hepting* held that the very subject matter of the claims in that action, which are similar to the claims in this action, is not a state secret. *Hepting*, 439 F.Supp.2d at 993-94.

That leaves the second and third *Mohamed* exceptions: the valid-defense exception and the unacceptable-risk exception. The government has not carried its burden under either of these two exceptions.

1. The Government Has Not Proven That The Privileged Evidence Demonstrates The Existence Of A Valid Defense

The government unsuccessfully attempts to invoke the valid-defense exception. In a single sentence unsupported by argument or explanation, the government conclusorily asserts that "even if plaintiffs could make out a prima facie case, the privilege would preclude defendants from presenting their defenses." Gov't Br. at 35-36. The government does not identify what these purported defenses are or assert that they have submitted secret evidence *in camera* sufficient to prove the existence of these defenses.

As *General Dynamics* makes clear, the valid-defense exception is contrary to the state secrets privilege as established in *Reynolds*, under which as with any other privilege the evidence is excluded and the lawsuit proceeds regardless of which party is prejudiced by the exclusion. *General Dynamics*, 131 S.Ct. at 1906. For contract cases, *General Dynamics* sensibly grounds the valid-defense exception on the ability of the parties to a contract to allocate the risk that they will be unable to prove a contract breach because of the state secrets privilege. 131 S.Ct. at 1909. No similar basis exists for extending the rule to non-contract actions like this one based on constitutional and statutory violations.

In any event, the government has failed to meet the requirements of this exception. This exception requires that the excluded evidence make it impossible for the defendant to prove up a "*valid* defense." *Mohamed*, 614 F.3d at 1083 (italics added) (citing *In re Sealed Case*, 494 F.3d at 153). This is a high standard for a defendant to meet, and the government does not even attempt to do so: "A 'valid defense' . . . is meritorious and not merely plausible and would *require* judgment for the defendant. 'Meritorious,' in turn, means 'meriting a legal victory.'" *In re Sealed Case*, 494 F.3d at 149 (citations omitted, italics added).

To determine whether the proposed defense is meritorious and requires judgment for the defendant, the district court must examine the privileged evidence itself, not just declarations

asserting the privilege, and determine whether it proves the existence of the defense: "If the defendant proffers a valid defense that the district court *verifies upon its review of state secrets evidence*, then the case must be dismissed." *In re Sealed Case*, 494 F.3d at 153 (italics added); *accord*, *General Dynamics*, 131 S.Ct. at 1909-10 (dismissal permissible only if the "defense is supported by enough evidence to make out a prima facie case" (*id*. at 1909), *i.e.*, "enough evidence to survive summary judgment" (*id*. at 1910)). To avoid strategic assertions of the privilege, this verification must be especially searching when the government is not an intervenor but a defendant simultaneously withholding evidence under the privilege while seeking dismissal on the ground that it has thereby crippled itself from presenting a valid defense.

The District of Columbia Circuit has explained why the defense must be proven by the secret evidence to be "demonstrably valid" and not just "plausible:"

> Were the valid-defense exception expanded to mandate dismissal of a complaint for any plausible or colorable defense, then virtually every case in which the United States successfully invokes the state secrets privilege would need to be dismissed. This would mean abandoning the practice of deciding cases on the basis of evidence—the unprivileged evidence and privileged-but-dispositive evidence—in favor of a system of conjecture. . . . [I]t would be manifestly unfair to a plaintiff to impose a presumption that the defendant has a valid defense that is obscured by the privilege. There is no support for such a presumption among the other evidentiary privileges because a presumption would invariably shift the burdens of proof, something the courts may not do under the auspices of privilege.

In re Sealed Case, 494 F.3d at 149-50. The court continued: "[A]llowing the mere prospect of a privileged defense to thwart a citizen's efforts to vindicate his or her constitutional rights would run afoul of the Supreme Court's caution against precluding review of constitutional claims, *see Webster* [*v. Doe*], 486 U.S. [592,] 603-04 [(1988)], and against broadly interpreting evidentiary privileges . . . ." *In re Sealed Case*, 494 F.3d at 151.

The government has not even attempted to make the necessary showing here to trigger the valid-defense exception. It has not submitted to the Court any privileged evidence, as opposed to declarations asserting that evidence exists that is privileged. It has not identified any affirmative defense that is valid, or even one that is merely plausible. It has not attempted to rebut plaintiffs' evidence, including the Klein and Marcus declarations. The valid-defense exception, even if it

applied to non-contract cases, thus provides no basis for dismissing plaintiffs' lawsuit.

2. Litigation Using Only Non-Privileged Evidence Will Not Reveal State Secrets

The third *Mohamed* exception permitting threshold dismissal is where litigation of the action using only non-privileged evidence inevitably "would create an unjustifiable risk of revealing state secrets." *Mohamed*, 614 F.3d at 1088. For a risk to be "unjustifiable" it must be more than the merely theoretical risk of disclosure that exists in every case that touches on state secrets, or else *every* states secrets invocation would require automatic dismissal and there would be nothing left of *Reynolds* and the rule that "the privileged information is excluded and the trial goes on without it." *General Dynamics*, 131 S.Ct. at 1906. The government contends that "this is one of those rare cases" in which litigation of the action using only non-privileged evidence inevitably would create an unjustifiable risk of revealing state secrets. *Mohamed*, 614 F.3d. at 1092.

The government never explains why, once any properly privileged evidence is excluded from the case and not disclosed, there will nonetheless remain an unjustifiable risk of revealing state secrets. Its brief says the Clapper and Fleisch declarations identify the information at risk of disclosure even if the privilege is applied, but the government nowhere describes the mechanism by which the disclosure it hypothesizes might occur. Gov't Br. at 24. The Clapper Declaration identifies only one category of information at risk of disclosure, information about whether NSA obtains communications records in bulk from AT&T. Clapper Decl. ¶ 25. DNI Clapper, however, identifies this risk as occurring if *NSA* "confirm[s]or deni[es]" the information. If the information is properly subject to the privilege, there will be no confirmation or denial by the NSA and therefore no risk of disclosure; if the information is not a secret properly subject to withholding by the NSA under the privilege, then what is at risk of disclosure is not a secret. The Fleisch Declaration asserts that information related to the government's alleged defenses would risk disclosure of NSA sources and methods, Fleisch Decl. ¶ 19, but that contention is properly addressed under the valid-defense exception discussed above. If the defense is not valid, the government will have no need to introduce any evidence, secret or otherwise, in support of it.

III. The Government's Sovereign Immunity Arguments Lack Merit

The government argues that sovereign immunity shields them against plaintiffs' claims both for damages and for equitable relief. The government is wrong on both counts.

A. Congress Waived Sovereign Immunity For Plaintiffs' Damages Claims[8]

Congress has expressly waived sovereign immunity for damages claims for violations of the Wiretap Act and the SCA by the plain language of 18 U.S.C. § 2712(a), which authorizes suits against the United States for *any* willful violation of those statutes. Section 2712 is plain and unambiguous:

> Any person who is aggrieved by any willful violation of this chapter [the SCA] **OR** of chapter 119 of this title [the Wiretap Act**] OR** of sections 106(a), 305(a), or 405(a) of [FISA] may commence an action in United States District Court against the United States to recover money damages.

18 U.S.C. § 2712(a) (capitalization and emphasis added).

Ignoring this plain language, the government makes frivolous argument that Section 2712's waiver of sovereign immunity does not actually reach surveillance in violation of these laws. Instead, the government argues that the waiver is limited to violations of a few specific Wiretap Act and ECPA provisions that regulate the government's *use or disclosure* of information obtained pursuant to those statutes, *i.e.*, 18 U.S.C. §§ 2520(g) and 2707(g). *See* Gov't Br. at 5-6.

The government's argument is directly counter to Section 2712's plain and unambiguous statement that the United States is subject to suit for "*any* willful violation" of the Wiretap Act or the SCA, which is as express and unequivocal as a waiver could be. If Congress had wished to limit Section 2712's waiver to particular provisions of the Wiretap Act or the SCA, "it knew how to do so." *Custis v. United States*, 511 U.S. 485, 492 (1994). Indeed, Congress placed specific limits on FISA causes of action *in the very same sentence*, waiving sovereign immunity only as to specific provisions of FISA. *See* 18 U.S.C. § 2712(a). No similar limitation, however, was placed

[8] Plaintiffs acknowledge that in *Al-Haramain v. Obama*, 690 F.3d 1089 (9th Cir. Aug. 7, 2012), the Ninth Circuit held that 50 U.S.C. § 1810 does not waive sovereign immunity against the United States for damages. While plaintiffs dispute this issue for purposes of preserving their appellate rights, they acknowledge that this Court is bound by the Ninth Circuit's ruling with respect to plaintiffs' damages claims against the United States under § 1810. *See* Complaint, Count VI.

on Wiretap Act or SCA causes of action.

In an attempt to justify their argument that Congress has waived sovereign immunity only for "the use and disclosure" of information obtained through illegal surveillance, the government badly misconstrues *Al-Haramain v. Obama*, 690 F.3d at 1089. *See* Gov't Br. at 5-7. Contrary to the government's arguments, *Al-Haramain* does not discuss Section 2712's express waiver of sovereign immunity for violations of the Wiretap Act or the SCA at all much less limit them to only "use and disclosure" claims. Rather, as *Al-Haramain* explained, the "use and disclosure" limitations for FISA claims arise from the language of the FISA sections specifically enumerated in Section 2712, not from Section 2712 itself. *Id.* at 1096, 1098 & n.3. 50 U.S.C. § 1806(a), for example, limits how "[i]nformation acquired from an electronic surveillance" "may be used and disclosed." The Ninth Circuit in *Al-Haramain* recognized that Section 2712 "*explicitly* waives sovereign immunity." *Id.* at 1098 (italics in original). That explicit waiver by its terms extends to any willful violation of *any* provision of the Wiretap Act or the SCA.

Other provisions of Section 2712 independently foreclose the government's argument. As explained in Section I(A)(1) above, Section 2712(b)(4) provides that Section 1806(f) applies to actions brought under Section 2712. Section 1806(f) requires the court "to determine *whether the surveillance of the aggrieved person was lawfully authorized and conducted*." 50 U.S.C. § 1806(f) (italics added). If the government was correct that the United States cannot be sued under Section 2712 for Wiretap and SCA violations involving unlawful surveillance, but only for unlawful disclosures of surveillance-derived information, Section 2712(b)(4)'s direction to use Section 1806(f) to determine the legality of the surveillance in the Wiretap Act and SCA would be purposeless. *Duncan,* 533 U.S. at 174 (courts must "give effect, if possible, to every clause and word of a statute").

The government willfully misreads the statute and legislative history when it counters that a plain language reading of Section 2712's sovereign immunity waiver should be abandoned in favor of a "holistic" look at Section 223 of the USA PATRIOT Act's other amendments to the Wiretap Act and the SCA. Gov't Br. at 8; USA PATRIOT Act of 2001, Pub L. No. 107-56, 115 Stat. 272 ("PATRIOT") at § 223(a)(1), (b)(1). Congress's purpose was not to eliminate all causes of action

against the government for surveillance in violation of those statutes. Instead, it modified the pre-existing causes of action under 18 U.S.C. sections 2520 (for Wiretap Act violations) and 2707 (for SCA violations), which applied to persons or entities generally, by separating out suits against the United States into a new cause of action under Section 2712 that provided new procedures and requirements specific to those suits. In doing so, Congress used statutory language that waived sovereign immunity for *"**any** willful violation"* of the SCA or the Wiretap Act. 18 U.S.C. § 2712 (emphasis added).

The government's resort to legislative history is both unnecessary and improper, because the plain language of Section 2712 is clear. *See Mohamad v. Palestinian Auth.,* 132 S.Ct. at 1709. Nonetheless, none of the history cited by the government supports its argument that Congress intended Section 2712 to waive sovereign immunity *only* against claims for unauthorized disclosures. Rather, that history confirms that a waiver for disclosure claims was *one* of that section's purposes. *See* Gov't Exs. 2-4.[9]

B. Sovereign Immunity Does Not Bar Plaintiffs' Equitable Claims

1. Plaintiffs' "*Ultra Vires*" Claims Alleging The Government Officer Defendants Lack Authority To Conduct Dragnet Surveillance Are Not Claims Against The United States And Thus Cannot Be Barred By Sovereign Immunity

Plaintiffs' equitable relief claims against the federal officer defendants are sound because

---

[9] In fact, the government's pre-litigation interpretation of the breadth of Section 2712's waiver of sovereign immunity is directly contrary to the version they now espouse. The Justice Department's own surveillance manual warns government agents that they may be liable for unauthorized disclosures under Section 2712 *in addition* to being liable for illegal surveillance:

> Although ECPA does not provide a suppression remedy for statutory violations, it does provide for civil damages . . . against officers and employees of the United States who have engaged in willful violations of the statute. Liability and discipline can result *not only* from violations of the rules already described in this chapter [*i.e.*, ECPA's rules governing government access to content and records stored by electronic communication service providers], but *also* from the improper disclosure of some kinds of ECPA-related information.

U.S. Dep't of Justice, Searching & Seizing Computers & Obtaining Elec. Evid. in Crim. Investigations, Section 2, at 109-110, attached to Opsahl Decl., Exh. 62 (emphasis added).

they are based on "*ultra vires*" conduct that violates the statutory limits on the authority of those officers. *Larson v. Domestic & Foreign Commerce Corp.*, 337 U.S. 682, 689-90 (1949). Counts V, VII, X, and XIII seek equitable relief against government officer defendants Alexander, Holder, and Clapper on the grounds that they lack statutory authority for the dragnet surveillance they are conducting and that they are exceeding statutory limitations on their authority. Plaintiffs seek equitable relief to confine the actions of these government officer defendants within the statutory limits of their offices. (Defendants do not contest that Counts I, III, and XVII properly state claims for equitable relief against them for constitutional violations.)

The government's argument that sovereign immunity bars these claims ignores the fact that these *ultra vires* claims against government officers are not claims against the United States to which sovereign immunity attaches. An equitable relief claim to restrain a federal officer from exceeding the powers he or she has been granted by statute—an *ultra vires* claim—is not a claim against the United States, and for that reason it is not barred by sovereign immunity. As the D.C. Circuit (the court that most regularly reviews the lawfulness of executive action) has explained, in an *ultra vires* claim under *Larson* "there is no sovereign immunity to waive—it never attached in the first place." *Chamber of Commerce v. Reich*, 74 F.3d 1322, 1329 (D.C. Cir. 1996).

The dividing line, as the Supreme Court explained in *Larson*, is whether the claim alleges acts by the officer that, even if wrongful, are within the scope of the authority Congress has granted or instead alleges acts by the officer beyond the limits of his or her authority. 337 U.S. at 690. Only "if the actions of an officer do *not* conflict with the terms of his valid statutory authority, . . . are [they] the actions of the sovereign" and subject to sovereign immunity. *Id*. at 695 (italics added). Otherwise, "the conduct against which specific relief is sought is beyond the officer's powers and is, therefore, not the conduct of the sovereign," and sovereign immunity does not apply. *Id*. at 690.

As *Larson* explains:

> where the officer's powers are limited by statute, his actions beyond those limitations are considered individual and not sovereign actions. The officer is not doing the business which the sovereign has empowered him to do or he is doing it in a way which the sovereign has forbidden. His actions are *ultra vires* his authority and therefore may be made the object of specific relief. It is important to note that in such cases the relief can be granted, without impleading the sovereign, only because of the officer's lack of delegated power.

Id. at 689-90. Because actions taken beyond the limits set by Congress are not those of the sovereign, enjoining the officer from transgressing those limits does not enjoin any act of the sovereign and does not interfere with the authority or impose upon the discretion of the sovereign. Indeed, it is the sovereign that has imposed the statutory limits upon the officer that the officer is transgressing.

Thus, "under *Larson* . . ., if the federal officer, against whom injunctive relief is sought, allegedly acted in excess of his legal authority, sovereign immunity does not bar a suit." *Chamber of Commerce v. Reich*, 74 F.3d at 1329; *accord*, *Harmon v. Brucker*, 355 U.S. 579, 581-82 (1958) (explaining "judicial relief is available to one who has been injured by an act of a government official which is in excess of his express or implied powers"); *Philadelphia Co. v. Stimson*, 223 U.S. 605, 620, 621-22 (1912) (explaining that "in case of an injury threatened by his illegal action, the officer cannot claim immunity from injunction process. . . . [when] acting in excess of his authority," and that "there may exist ground for equitable relief, when an officer, insisting that he has the warrant of the statute, is transcending its bounds, and thus unlawfully assuming to exercise the power of government against the individual"). For example, in *Harmon v. Brucker*, the Secretary of the Army had issued dishonorable discharges to the plaintiffs based on conduct occurring before their military service began. 355 U.S. at 580. Because the Secretary's statutory authority limited his power to issue dishonorable discharges to instances of dishonorable conduct occurring during military service, the Secretary's actions were in excess of his authority and the plaintiffs were entitled to injunctive relief directing the Secretary to issue them honorable discharges. *Id*. at 582-83.

Here, plaintiffs' complaint alleges *ultra vires* acts by the government officer defendants, *i.e.*, a program of dragnet surveillance that the officers lack any power to conduct and that reaches far beyond the narrow statutory limits Congress has imposed on them in the Wiretap Act, the SCA, and FISA. The complaint alleges the factual details of the dragnet content and records surveillance program and explains defendants' control of and participation in the program. Complaint ¶¶ 7-11, 39-49, 50-81, 82-97. Counts V, VII, X, and XIII allege that, by participating in the dragnet surveillance program, government officer defendants Alexander, Holder, and Clapper have acted in

excess of their statutory authority, exceeding the limits that the Wiretap Act, the SCA, and FISA place on their authority. Complaint ¶¶ 76-79, 92-95, 150-51, 154-55, 177, 181-82, 214, 218-19, 237, 241-42. For example, the complaint alleges that "[b]y the acts alleged herein, Defendants acting in excess of their statutory authority . . . have intentionally engaged in . . . electronic surveillance . . . not authorized by any statute" and that "by the acts alleged herein, Defendants acting in excess of their statutory authority and in violation of statutory limitations have intentionally disclosed or used information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance not authorized by statute." Complaint ¶¶ 150-51. Counts V, VII, X, and XIII thus are proper *ultra vires* claims to which sovereign immunity does not attach, because they allege each "officer's lack of delegated power" rather than "error in the exercise of that power." *See Larson*, 337 U.S. at 689-90.

Nor do the statutes the government cites foreclose equitable relief against federal officers for *ultra vires* conduct. 18 U.S.C. §§ 2520 and 2707 authorize suits for equitable relief against "persons," a term expressly including employees of the United States like government officer defendants Alexander, Holder, and Clapper; the statutes do not purport to exclude *Larson ultra vires* claims. 18 U.S.C. § 2510(6) ("any employee, or agent of the United States"); 18 U.S.C. § 2711(a) (same). Section 2712 addresses only claims against the United States, which an *ultra vires* claim is not. Finally, 50 U.S.C. § 1810 does not purport to forbid *ultra vires* suits against government officers and does not purport to make damages the exclusive remedy for FISA violations. Nor does the government point to any legislative history or other evidence of congressional intent to preclude *ultra vires* suits under the Wiretap Act, the SCA, and FISA.

The government's contention that Section 702 of the APA, 5 U.S.C. § 702, precludes all *ultra vires* actions against government officers and somehow abrogated *Larson* is nonsense. *See Chamber of Commerce v. Reich*, 74 F.3d at 1328-29 (applying *Larson* after enactment of Section 702). The whole purpose of Section 702, discussed further in the next section, is to waive sovereign immunity to make it *easier* to bring claims against the government and government officers alleging constitutional and statutory violations and seeking equitable relief. The idea that it

silently abrogated *Larson* and *narrowed* the ability of plaintiffs to bring such suits is unfounded. The statutory text is entirely permissive; it permits actions to be brought that in many cases sovereign immunity would otherwise bar. It does not forbid any suits that could otherwise be brought in its absence. In particular, it says nothing about *Larson* or *ultra vires* claims. Nor has the Supreme Court or the Ninth Circuit rejected *Larson*. The two Ninth Circuit decisions cited by the government were not cases in which the plaintiffs were seeking to rely on *Larson* to bring an *ultra vires* suit and neither held that a plaintiff cannot bring an *ultra vires* claim under *Larson*. The decisions simply recognize that Section 702 has largely "eliminated the need to invoke" *Larson*, not that Congress has abrogated *Larson*. *EEOC v. Peabody Western Coal Co.*, 610 F.3d 1070, 1086 (9th Cir. 2010); *Presbyterian Church (U.S.A.) v. U.S.*, 870 F.2d 518, 526 (9th Cir. 1989).

The government also errs in contending that compelling a federal officer to remain within the limits of his or her statutory authority interferes with the public administration. There is no public interest in unauthorized, lawless conduct by federal officials, and preventing lawless conduct advances, rather than interferes with, the public administration. As the Supreme Court has recognized, in a "suit against a public official who invades a private right . . . by exceeding his authority," "relief against the offending officer could be granted without risk that the judgment awarded would '. . . interfere with the public administration.' " *Williams v. Fanning*, 332 U.S. 490, 493 (1947). In *Dugan v. Rank*, 372 U.S. 609, 620-22 (1963), the Supreme Court reaffirmed that *Larson ultra vires* actions are "exceptions to the . . . general rule" regarding suits that might "interfere with the public administration," and remain outside the scope of sovereign immunity.

Finally, *Pennhurst State School & Hospital v. Halderman*, 465 U.S. 89 (1984), has no application here. That case involved efforts to obtain injunctive relief against *state*, not federal, officials to enforce *state*, not federal, law. In that context, the Supreme Court held that a federal court could not intrude upon state sovereignty by enjoining state officials for failing to meet state standards of care in operating a state hospital. *Pennhurst,* 465 U.S. at 106. The federalism, Eleventh Amendment, and Supremacy Clause questions involved in determining the circumstances

under which a federal court can impinge on state sovereignty by ordering injunctive relief against state officers do not apply in actions like this one alleging *ultra vires* conduct by federal officers.[10]

2. Congress Waived Sovereign Immunity For Plaintiffs' Equitable Relief Claims, Including Plaintiffs' APA Claim

Independently, Section 702 of the Administrative Procedures Act waives sovereign immunity for claims against government agencies and officers seeking equitable relief. 5 U.S.C. § 702 (waiving sovereign immunity for suits "seeking relief other than money damages and stating a claim that an agency or an officer or employee thereof acted or failed to act in an official capacity or under color of legal authority "). Section 702's waiver applies both to claims brought under provisions of the APA like Section 704 and to claims brought outside the APA to enforce other statutory or constitutional provisions. *Trudeau v. FTC*, 456 F.3d 178, 186 (D.C. Cir. 2006) (holding Section 702's "'waiver of sovereign immunity applies to any suit whether under the APA or not'"); *Presbyterian Church*, 870 F.2d at 525 (explaining "§ 702 waives sovereign immunity in all actions seeking relief from official misconduct"); *Assiniboine & Sioux Tribes v. Bd. of Oil & Gas*, 792 F.2d 782, 793 (9th Cir. 1986) (same).

Section 702's waiver applies to plaintiffs' APA cause of action in Count XVI, which seeks equitable relief under, *inter alia*, Sections 704 and 706 of the APA against the government agency defendants (the United States, the Department of Justice, and the NSA) and against government officer defendants Alexander, Holder, and Clapper for constitutional and statutory violations, including violations of the Fourth Amendment, the Wiretap Act, ECPA, the SCA, and FISA. Defendants present no argument supporting their contention that plaintiffs' APA cause of action is barred by sovereign immunity.

[10] Nor do the other cases the government cites support its contention that plaintiffs' *ultra vires* claims are barred by sovereign immunity. *Central Reserve Life Ins. Co. v. Struve*, 852 F.2d 1158, 1160-61 (9th Cir. 1988), was a case seeking to enforce state law against state officials, and thus was barred by *Pennhurst.* In *Aminoil U.S.A., Inc. v. California State Water Resources Control Bd.*, 674 F.2d 1227, 1234 (9th Cir. 1982), the Ninth Circuit found that the challenged conduct was within the federal official's statutory authority and not *ultra vires. Palomar Pomerado Health System v. Belshe*, 180 F.3d 1104, 1108 (9th Cir. 1999), was a suit against state officials with no allegation of *ultra vires* conduct.

Section 702 also waives any possible sovereign immunity defense to Counts V, VII, X, and XIII, which are brought only against the government officer defendants (even though, for the reasons stated in the preceding section, there is no sovereign immunity defense to those claims and thus no need for a waiver). *Trudeau*, 456 F.3d at 186; *Presbyterian Church*, 870 F.2d at 525. Defendants contend, however, that Section 702's waiver does not apply to plaintiffs' equitable relief claims in Counts V, VII, X, and XIII, which allege violations of the Wiretap Act, the SCA, and FISA. In support of that contention, defendants rely on an exception to Section 702's sovereign immunity waiver that applies "if any other statute that grants consent to suit expressly or impliedly forbids the relief which is sought." 5 U.S.C. § 702.

Defendants' argument lacks merit. The exception to Section 702 requires defendants to identify a statute that both (1) grants consent to suit against the United States (*i.e.*, waives sovereign immunity) for the claims alleged and (2) forbids equitable relief. No such statute exists.

Defendants are mistaken in contending that Section 2712(a) bars equitable relief for FISA violations (Count V). Section 2712(a) does not grant consent to suit for violations of 50 U.S.C. § 1809 of FISA—the provision that plaintiffs sue under. Instead, it grants consent to suit for violations of other, unrelated provisions of FISA having to do not with the acquisition of communications but with the unauthorized *use or disclosure* of: lawfully intercepted communications (50 U.S.C. § 1806(a)); information gathered in physical searches (50 U.S.C. § 1825(a)); or information gathered using pen registers (50 U.S.C. § 1845(a)).

Section 2712(a) thus fails the first prong of the exception to APA Section 702: it is not a "statute that grants consent to suit" for plaintiffs' 50 U.S.C. § 1810 FISA claim. 5 U.S.C. § 702. As the Supreme Court recently affirmed, Section 702's sovereign immunity waiver is not negated by a statute granting the right to sue for a "grievance different from the one [the plaintiff] advances." *Match-E-Be-Nash-She-Wish Band of Pottawatomi Indians v. Patchak*, __ U.S. __, 132 S.Ct. 2199, 2206 (2012). Because in Count V plaintiffs are "bringing a different claim, seeking different relief" than the particular FISA claims listed in Section 2712(a), Section 2712(a) does not negate APA Section 702's sovereign immunity waiver. *Patchak*, 132 S.Ct. at 2209.

The first two statutes that defendants assert bar equitable relief for Wiretap Act and SCA violations (Counts VII, X, and XIII), 18 U.S.C. §§ 2520(a) and 2707(a), similarly do not grant consent to suit against the United States for Wiretap Act and SCA violations, so they do not meet the first prong of the exception to Section 702. The third statute, 18 U.S.C. § 2712, does grant consent to suit against the United States, but it does not meet the second prong because it does not forbid equitable relief. Section 2712 provides that it is "the exclusive remedy against the United States for any claims *within the purview* of this section." 18 U.S.C. § 2712(d) (italics added). The purview of Section 2712 is set forth in subsection (a) as "an action . . . against the United States to recover money damages." Section 2712 sets the parameters regarding those damages claims, such as requiring the claims to be in excess of $10,000 and making available litigation costs as an additional remedy. 18 U.S.C. § 2712. Thus, only damages claims, and not equitable relief claims, are "within the purview" of Section 2712. Section 2712 therefore provides the exclusive avenue for monetary relief and forbids any other claim for money damages, but does not forbid equitable relief. Plaintiffs' claims for equitable relief for violations of the Wiretap Act and SCA are "different claim[s], seeking different relief." *Patchak,* 132 S.Ct. at 2209.[11]

When Congress enacted FISA in 1978, after APA Section 702's enactment, it intended the statutory limits of FISA to be enforceable by the courts. Congress provided that FISA, the Wiretap Act, and ECPA together are the exclusive means by which electronic surveillance may be conducted. 18 U.S.C. § 2511(2)(f); 50 U.S.C. § 1812(a). Congress's command that surveillance may only be conducted within the narrow limitations of those three Acts would be illusory if judicial review were unavailable to enjoin violations of those Acts by the government.

CONCLUSION

Plaintiffs' motion for partial summary judgment should be granted and the government defendants' motion to dismiss or for summary judgment should be denied.

[11] By contrast, the statute in *Block v. North Dakota*, 461 U.S. 273, 286 n.22 (1983), cited by the government, both granted consent to suit and expressly forbade the relief the plaintiff sought.

DATE: October 9, 2012

Respectfully submitted,

s/ Richard R. Wiebe

CINDY COHN
LEE TIEN
KURT OPSAHL
JAMES S. TYRE
MARK RUMOLD
ELECTRONIC FRONTIER FOUNDATION

RICHARD R. WIEBE
LAW OFFICE OF RICHARD R. WIEBE

THOMAS E. MOORE III
THE MOORE LAW GROUP

RACHAEL E. MENY
PAULA L. BLIZZARD
MICHAEL S. KWUN
AUDREY WALTON-HADLOCK
KEKER & VAN NEST LLP

ARAM ANTARAMIAN
LAW OFFICE OF ARAM ANTARAMIAN

Attorneys for Plaintiffs