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

RICHARD R. WIEBE (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

RACHAEL E. MENY (178514)
rmeny@kvn.com
PAULA L. BLIZZARD (207920)
MICHAEL S. KWUN (198945)
AUDREY WALTON-HADLOCK (250574)
KEKER & VAN NEST, LLP
710 Sansome Street
San Francisco, California 94111-1704
Telephone: (415) 391-5400
Fax: (415) 397-7188

THOMAS E. MOORE III (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 (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' MOTION FOR PARTIAL SUMMARY JUDGMENT REJECTING THE GOVERNMENT DEFENDANTS' STATE SECRET DEFENSE

Date: November 2, 2012
Time: 9:00 a.m.
Courtroom 11, 19th Floor
The Honorable Jeffrey S. White

TABLE OF CONTENTS

I. Introduction 2

II. Statement Of Facts 3

A. The Klein Evidence, AT&T's Confirmation, And The Marcus Expert Declaration 3

B. The President's Surveillance Program 6

III. Issues For Decision 9

IV. Section 1806(f) Displaces The State Secrets Privilege In Lawsuits Alleging Unlawful Electronic Surveillance 9

A. The State Secrets Privilege 10

B. Congress Has Displaced The State Secrets Privilege With Section 1806(f) In Cases Involving Electronic Surveillance 12

C. FISA's Statutory Scheme And Legislative History Confirm That Section 1806(f) Displaces The State Secrets Privilege 14

1. Congress Enacted FISA To Establish Comprehensive Control Over National Security Electronic Surveillance 14

2. Section 1806(f) Is An Essential Element Of Congress' Comprehensive Scheme For Judicially Enforcing The Limitations It Has Imposed On Electronic Surveillance 16

V. Section 1806(f) Directs This Court To Determine Whether Defendants Subjected Plaintiffs To Unlawful Surveillance 18

VI. Conclusion 22

TABLE OF AUTHORITIES

Cases

Al-Haramain Islamic Foundation, Inc. v. Bush ("*Al-Haramain I*"), 507 F.3d 1190 (9th Cir. 2007) 10, 12, 19

Beck v. Prupis, 529 U.S. 494 (2000) 20

General Dynamics Corp. v. United States, __ U.S. __, 131 S.Ct. 1900 (2011) 10, 11

Golinski v. U.S. Office of Personnel Management, 824 F. Supp. 2d 968 (N.D. Cal. 2012) 10, 11

Hepting v. AT&T Corp., 439 F. Supp. 2d 974 (N.D. Cal. 2006) 6

In re National Security Agency Telecommunications Records Litigation (*Al-Haramain Islamic Foundation, Inc. v. Bush*), 564 F. Supp. 2d 1109 (N.D. Cal. 2008) 12

In re Sealed Case, 494 F.3d 139 (D.C. Cir. 2007) 11

Jewel v. NSA, 673 F.3d 902 (9th Cir. 2011) 2, 3, 21

Kasza v. Browner, 133 F.3d 1159 (9th Cir. 1998) 10

Mohamed v. Jeppesen Dataplan, Inc., 614 F.3d 1070 (9th Cir. 2010) (en banc) 10, 11

Morissette v. United States, 342 U.S. 246 (1952) 20

Totten v. United States, 92 U.S. 105 (1876) 10, 11

United States v. Reynolds, 345 U.S. 1 (1953) 10, 11

Usery v. Turner Elkhorn Mining Co., 428 U.S. 1 (1976) 13

Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579 (1952) 15

Statutes

18 U.S.C. § 2511(2)(f) 16

50 U.S.C. § 1801 ..... 16, 1
50 U.S.C. § 1801(f)(2) 18
50 U.S.C. § 1801(k) 19, 21
50 U.S.C. § 1801(n) 18
50 U.S.C. § 1804 ..... 7, 16
50 U.S.C. § 1806(e) 17
50 U.S.C. § 1806(f) ..... passim
50 U.S.C. § 1809 17
50 U.S.C. § 1810 ..... 17, 19
50 U.S.C. § 1811 7
50 U.S.C. § 1812 16
Classified Information Procedures Act, 18 U.S.C. App. 3 18
Foreign Intelligence Surveillance Act of 1978, Pub. L. 95-511, 92 Stat. 1783 17
Pub. L. No. 93-595, 88 Stat. 1933 14
Stored Communications Act, 18 U.S.C. §§ 2701-2712 ..... 2, 16, 17
Wiretap Act, 18 U.S.C. §§ 2510-2522 ..... 2, 16, 17

Rules

Federal Rule of Civil Procedure 11 21
Federal Rule of Civil Procedure 26 ..... 20, 21
Federal Rule of Civil Procedure 56 10
Federal Rule of Evidence 501 ..... 13, 14

Executive Materials

Offices of Inspectors General, *Unclassified Report On The President's Surveillance Program* (July 2009) (available at www.dni.gov/reports/report_071309.pdf) 7, 8

Legislative Materials

H.R. Conf. Rep. No. 95-1720 (1978),
reprinted in 1978 U.S.C.C.A.N. 4048 (FISA House-Senate Conference Report) 17

H.R. Rep. No. 93-650 (1973),
reprinted in 1974 U.S.C.C.A.N. 7075 14

H.R. Rep. No. 95-1283 (1978) 19

S. Rep. No. 93-1277 (1974),
reprinted in 1974 U.S.C.C.A.N. 7051 14

S. Rep. No. 94-1035 (1976) 16

S. Rep. No. 95-604(I) (1978),
reprinted in 1978 U.S.C.C.A.N. 3904 ..... 15, 16, 17

S. Rep. No. 95-701 (1978)
reprinted in 1978 U.S.C.C.A.N. 3973 20

S. Select Comm. to Study Governmental Operations with Respect to Intelligence Activities,
Book II: Intelligence Activities and the Rights of Americans,
S. Rep. No. 94-755 (1976) (available at
http://www.aarclibrary.org/publib/contents/church/contents_church_reports.htm) 7, 15

Other Sources

James Risen & Eric Lichtblau, *Bush lets U.S. spy on callers without courts*,
New York Times, December 16, 2005,
(available at http://www.nytimes.com/2005/12/16/politics/16program.html) 8

Leslie Cauley, *NSA has massive database of Americans' phone calls*,
USA Today, May 11, 2006,
(available at http://www.usatoday.com/news/washington/2006-05-10-nsa_x.htm) 8

Matthew D. Laplante, *Spies like us: NSA to build huge facility in Utah*,
Salt Lake Tribune, July 1, 2009,
(available at http://www.sltrib.com/ci_12735293) 9

NOTICE OF MOTION AND MOTION FOR PARTIAL SUMMARY JUDGMENT

PLEASE TAKE NOTICE that on November 2, 2012 at 9:00 a.m. in Courtroom 11, 19th Floor, United States District Court, 450 Golden Gate Ave., San Francisco, CA, plaintiffs will move for partial summary judgment holding that the state secrets privilege defense of defendants National Security Agency, United States, Department of Justice, Barack H. Obama, Keith B. Alexander, Eric H. Holder, Jr., and James R. Clapper, Jr. (in their official capacities) (collectively, the "government defendants") lacks merit.[1]

The ground for this motion is that Congress has displaced the state secrets privilege in this action by the statutory procedure of 50 U.S.C. § 1806(f) of the Foreign Intelligence Surveillance Act. Under section 1806(f), which applies to electronic surveillance lawsuits like this one, Congress explicitly provided for courts to determine the legality of electronic surveillance, and provided for the discovery and use of national security evidence under secure conditions. Plaintiffs' motion is based on the accompanying memorandum, the declarations of Mark Klein, J. Scott Marcus, James W. Russell, William Binney, Thomas Drake, J. Kirk Wiebe, and Cindy A. Cohn, the filings and pleadings of record in this action and the related action of *Hepting v. AT&T* (U.S.D.C. N.D. Cal. No. 06-CV-0672),[2] and the argument and evidence presented at the hearing of this motion.

[1] As an accommodation to the government defendants, plaintiffs have noticed the hearing for this motion for November 2, 2012. The parties have agreed to a stipulation and proposed order, filed herewith, setting out a briefing schedule in which the government's response is due on August 31, 2012 and addressing several other matters.

[2] This action is related to the *Hepting* action, which was brought only against AT&T and not against any government entity or employee. Four of the plaintiffs here were also plaintiffs in *Hepting*. *Hepting* was dismissed in 2009 pursuant to a grant of immunity to AT&T by the Attorney General; none of the *Hepting* plaintiffs' claims was ever decided on its merits. The immunity dismissal was affirmed by the Ninth Circuit and the *Hepting* plaintiffs currently have a petition for certiorari pending. Although *Hepting* was a part of a multi-district litigation consolidating over 30 case for pretrial proceedings (MDL No. 06-CV-1791), this action has never been a part of the MDL.

MEMORANDUM

I. Introduction

This action arises out of the United States government's program of warrantless, untargeted, domestic mass surveillance that has intercepted the communications and communications records of millions of innocent Americans, including plaintiffs. Essentially, the case asks a simple but fundamental question: is it lawful or constitutional for the government to divert to its control a copy of the everyday communications and the trail of communications records of ordinary Americans not suspected of any connection to crime or terrorism?

In order to answer this question and to seek appropriate relief for the illegal surveillance of their personal communications, plaintiffs—customers of AT&T for whom compelling evidence exists of this mass surveillance—have sued the United States and government officials in their official and individual capacities, stating claims under the Fourth and First Amendments, the Foreign Intelligence Surveillance Act (FISA), the Wiretap Act, the Stored Communications Act provisions of the Electronic Communications Privacy Act, the Administrative Procedures Act, and the separation of powers doctrine. Dkt. #1.

In enacting the statutory procedure of 50 U.S.C. § 1806(f), Congress displaced the state secrets privilege in electronic surveillance actions. Both FISA and the state secrets privilege address judicial treatment of national security materials. Under FISA, which applies to electronic surveillance lawsuits, the secret evidence is put before the court, and the court must address the merits, including the legality of the electronic surveillance. Under the state secrets privilege, the secret evidence is excluded from consideration, and a plaintiff can only move the case forward on the merits without the secret evidence.

In past proceedings in this action, the government defendants brought a motion to dismiss or in the alternative for summary judgment based on the state secrets privilege and sovereign immunity. Dkt. #18, #29, #31. Without deciding that motion, the district court, per Walker, C.J., *sua sponte* dismissed this action for lack of standing. Dkt. #57. The Ninth Circuit reversed the dismissal and remanded. *Jewel v. NSA*, 673 F.3d 902, 913 (9th Cir. 2011). As part of its order of remand, the Ninth Circuit directed this Court to decide "the government's assertion that the state

secrets privilege bars this litigation." *Id*. at 913-14. Plaintiffs make this motion to present the issue to the Court, pursuant to the Ninth Circuit's direction.

Section 1806(f), enacted in 1978 as part of FISA's comprehensive regulation of electronic surveillance, expressly applies "notwithstanding any other law," including the state secrets privilege. 50 U.S.C. § 1806(f) (hereafter, "§1806(f)" or "section 1806(f)"). It provides that the court shall "determine whether the surveillance of the aggrieved person was lawfully authorized and conducted" by using specific secure procedures, including *in camera* and *ex parte* proceedings, in the event the government claims that the disclosure of certain evidence may potentially harm the national security of the United States. § 1806(f). Accordingly, the state secrets privilege is inapplicable here as a matter of law.

II. Statement Of Facts

Plaintiffs are customers of AT&T whose electronic communications and communications records have been unlawfully intercepted and disclosed to the government as part of a larger program of warrantless, untargeted domestic surveillance. Among the non-secret evidence demonstrating the electronic surveillance of plaintiffs is the detailed eyewitness testimony and documentary evidence of Mark Klein, a retired AT&T employee, and the expert testimony of J. Scott Marcus, an expert in telecommunications networks. Klein disclosed that AT&T and the NSA had installed powerful equipment at an AT&T facility in San Francisco and elsewhere, equipment designed to intercept both international and domestic electronic communications, including those of plaintiffs. Subsequent to Klein's disclosures, other evidence has emerged that both confirms Klein's evidence, adds additional facts, and places Klein's evidence into the broader context of a group of unlawful intelligence activities dubbed the President's Surveillance Program ("PSP").

A. The Klein Evidence, AT&T's Confirmation, And The Marcus Expert Declaration

Klein worked as an AT&T technician for 22 years, most recently at AT&T's San Francisco facilities. In a sworn declaration, he described events and operations he observed at AT&T demonstrating that AT&T has been collaborating with the National Security Agency ("NSA") in

the surveillance of the domestic communications of millions of Americans, including AT&T customers like plaintiffs.

Klein's account begins around January 2003, when the manager of his facility advised him that the NSA was coming to interview another colleague for a "special job" installing equipment in a high-security room AT&T was building for the NSA at its Folsom Street Facility in San Francisco—the "SG3" room. Klein Decl., ¶¶ 10-14. Klein personally saw the NSA's SG3 room when it was under construction, and, at one point, entered the room briefly after it was fully operational. *Id*., ¶¶ 12, 17. The AT&T employees in charge of the SG3 room had NSA security clearances. *Id*., ¶ 17.

In October 2003, AT&T transferred Klein to the Internet room at the Folsom Street Facility. Klein Decl., ¶ 15. Internet communications are carried as light signals on fiber-optic cables. *Id*., ¶¶ 21-22. Klein's job was to oversee the room containing the fiber-optic cables and switches carrying AT&T's Internet traffic. *Id*., ¶ 15. Communications carried by AT&T's Internet service pass through that room to be directed to or from customers. *Id*., ¶ 19. The room also contains connections between AT&T and the Internet networks of other Internet providers, so-called "peering links." *Id*., ¶¶ 29-33.

To divert the Internet communications traveling over its networks and other networks to the NSA, AT&T connected the fiber-optic cables of the peering links in the Internet room overseen by Klein to a "splitter cabinet" installed in the Internet room. *Id*., ¶¶ 28-34. The splitter cabinet splits the light signals in two, making two identical copies of all of the data carried on the light signal. *Id*., ¶¶ 23-25. The splitter cabinet directed one copy of the light signal through fiber-optic cables into the NSA's SG3 room while allowing the other copy to travel its normal course to its intended destination. *Id*., ¶ 27. All of the light signals on the fiber-optic cables of the peering links of AT&T's Internet network are copied and diverted to the NSA's SG3 room by the splitter equipment. *Id*., ¶¶ 19, 27, 29-34. The split cables carried domestic and international communications of AT&T customers, as well as communications from users of other non-AT&T networks that pass through the Folsom Street Facility. *Id*.

Klein attached to his declaration two AT&T documents called "SIMS Splitter Cut-In and

Test Procedure," which describe "how to connect the already in-service circuits to a 'splitter cabinet,' which diverted light signals from the WorldNet Internet service's fiber optical circuits to the SG3 Secure Room." Klein Decl., ¶¶ 25-26 & Exs. A, B. He also attached a third AT&T document "describ[ing] the connections from the SG3 Secure Room on the 6th floor to the WorldNet Internet room on the 7th floor, and provid[ing] diagrams on how the light signal was being split." *Id*., ¶ 28 & Ex. C. This document also "listed the equipment installed in the SG3 Secure Room," including a NARUS "Semantic Traffic Analyzer."[3] *Id*., ¶ 35. These three documents comprise over 100 pages of highly technical details on the interceptions, including 57 detailed schematics and 24 tables of data.

Klein further presented evidence that similar installations existed in other cities, including Atlanta, Seattle, San Jose, Los Angeles, and San Diego. Klein Decl., ¶ 36; Marcus Decl., ¶ 118.

James Russell, AT&T's Managing Director-Asset Protection, has confirmed that Klein's declaration and the AT&T documents Klein attached accurately describe AT&T's Internet network, AT&T's San Francisco communications facility, the location of specific equipment within the San Francisco facility, and the interconnection points of AT&T's Internet network with the networks of other communications carriers. Russell Decl. at ¶¶ 6, 10-12, 15, 19-22. Russell confirmed that the exhibits to the Klein Declaration are authentic AT&T documents that provide "detailed schematics of network wiring configurations that are uniform across AT&T locations and that are used by AT&T to cross-connect and split fiber cables" and "identif[y] the manufacturer and name of many pieces of equipment used by AT&T."[4] *Id*., ¶ 20.

Plaintiffs retained an expert in information technology and telecommunications to further explain the implications of the documents and testimony Klein furnished. The expert, J. Scott Marcus, spent decades working for a variety of telecommunications clients, including AT&T.

---

[3] The NARUS device collects Internet data at the rate of ten gigabytes per second and can reconstruct all information transmitted through it. It can also select data from the data stream according to predetermined criteria, such as target addresses, watch-listed names, keywords, etc., and can then forward on the selected information. Binney Decl., ¶ 10.

[4] Although the Russell declaration is under seal, AT&T, the proponent of its sealing in the *Hepting* action, has previously consented to the public disclosure of this summary of its contents.

Marcus Decl., ¶¶ 7-29. Marcus also served as the Senior Advisor for Internet Technology to the Federal Communications Commission. He concluded "that the room described was a secure facility, intended to be used for purposes of surveillance on a very substantial scale." *Id.*, ¶ 6. He "conclude[d] that AT&T has constructed an extensive—and expensive—collection of infrastructure that collectively has all the capability necessary to conduct large scale covert gathering of IP-based communications information, *not only for communications to overseas locations, but for purely domestic communications as well.*" *Id.*, ¶ 38 (emphasis in original). "This deployment *is neither modest nor limited*." *Id.*, ¶ 43 (emphasis in original). Marcus further concluded that AT&T made no effort to filter out purely domestic-to-domestic electronic communications, as a fiber splitter is not a selective device; all traffic on the split circuit was diverted or copied. *Id.*, ¶¶ 109-112.

The interceptions in San Francisco are not unique. Marcus concluded that AT&T's surveillance "apparently involves considerably more locations than would be required to catch the majority of international traffic." Marcus Decl., ¶ 43. According to Marcus, the web of surveillance facilities in cities such as Atlanta, Seattle, San Jose, and Los Angeles would probably capture well over half of AT&T's purely domestic traffic, representing almost all of the AT&T traffic to and from other providers. *Id.*, ¶ 124. The government has conceded that the Klein and Marcus evidence is not a state secret. *Hepting v. AT&T Corp.*, 439 F. Supp. 2d 974, 989 (N.D. Cal. 2006).

B. The President's Surveillance Program

Other public information about the government's surveillance activities supports the Klein and Marcus evidence, and provides broader context and background for plaintiffs' claims here. The NSA is the signals intelligence agency within the Department of Defense. Signals intelligence refers to intelligence gathering through the collection of signals such as electronic communications between persons such as radio transmissions, telephone signals and email, and the non-communications electronic emissions from equipment like radar. J. Kirk Wiebe Decl., ¶ 3.[5]

[5] William Binney, Thomas A. Drake, and J. Kirk Wiebe are former employees of the NSA and have submitted declarations in support of this motion. The information set forth in their

In 1976, the Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, better known as the "Church Committee," issued its report on the abuse of electronic surveillance by the NSA, along with the CIA and the FBI. S. Select Comm. to Study Governmental Operations with Respect to Intelligence Activities, *Book II: Intelligence Activities and the Rights of Americans*, S. Rep. No. 94-755 (1976). In response to the Church Committee report, Congress enacted FISA in 1978, expressly to provide the guidelines and limitations by which the agencies engaged in foreign intelligence might lawfully conduct electronic surveillance of communications transmitted between foreign and domestic locations, at time of peace (50 U.S.C. § 1804) and at time of war (50 U.S.C. § 1811).

Prior to September 11, 2001, the NSA treated FISA as a prime directive for lawfully conducting electronic surveillance for national security purposes in circumstances where one party to a communication was within the United States. The NSA managed that task while complying with FISA and instilling a respect for FISA among its employees. Drake Decl., ¶ 3; J. Kirk Wiebe Decl., ¶ 7; Offices of Inspectors General, *Unclassified Report On The President's Surveillance Program* (July 2009), at 4-5 (available at www.dni.gov/reports/report_071309.pdf) (hereafter "OIG", previously filed with the Court as Dkt. #35, Ex. A).

The attacks on September 11, 2001 prompted the White House to ask the NSA to reassess its intelligence-gathering capabilities not merely in terms of what was legally permissible but in terms of what was "operationally useful and technologically feasible." Binney Decl., ¶ 5; Drake Decl., ¶ 3; J. Kirk Wiebe Decl., ¶ 7; OIG at 5. The NSA responded with a variety of proposed intelligence-gathering activities. OIG at 5.

The NSA's response formed the basis of an extralegal Presidential authorization in October 2001 purporting to authorize a number of unlawful intelligence-gathering activities—later denominated collectively as the PSP. OIG at 5. The activities encompassed foreign intelligence-gathering, foreign-to-domestic intelligence-gathering and purely domestic intelligence-gathering. These activities were far more extensive than the limited subset of foreign-to-domestic al Qaeda-

---

declarations is all in the public domain, most notably set out in an article published in *The New Yorker* on May 23, 2011.

related electronic surveillance disclosed by the President in December 2005 that he called the "Terrorist Surveillance Program." OIG at 1-2, 5-6, 36-37; James Risen & Eric Lichtblau, *Bush lets U.S. spy on callers without courts*, New York Times, December 16, 2005 (available at http://www.nytimes.com/2005/12/16/politics/16program.html).

The NSA moved forward to implement the PSP, seizing vast amounts of data from millions of Americans. OIG at 14-15; Binney Decl., ¶ 5. Using tools like the NARUS, described above, the NSA had the capability to do individualized searches (similar to a Google search) for particular electronic communications through such criteria as target addresses, locations, countries and phone numbers, as well as watch-listed names, keywords, and phrases in email. The NSA also has, or is in the process of obtaining, the capability to store all electronic communications passing through the NSA's intercept centers, using tools like the fiber-optic splitter cabinet described above. The wholesale collection of data allows the NSA to identify and analyze intelligence from the electronic communications in a static database. But according to several retired NSA employees, the NSA did not have the technical capability to both protect the privacy of U.S. persons and collect and smartly select on the fly the nuggets of information it sought from the large volume of data traversing the Internet. Binney Decl., ¶¶ 5, 7, 9-13; Drake Decl., ¶¶ 7-10; J. Kirk Wiebe Decl., ¶¶ 8, 9. The NSA also asked for and received from AT&T and other telecommunications companies customer records of telephone calls made by millions of Americans.[6]

The NSA's interception infrastructure is consistent with these sweeping, untargeted seizures. The NSA could have chosen to limit its interception of electronic communications to international/international and international/domestic communications, thereby protecting the privacy of Americans in their domestic communications, by installing its intercept equipment only at the nation's foreign fiber-optic cable landing stations. There are more than two dozen cable landing sites on the U.S. coasts where fiber-optic cables come ashore. Instead, the NSA chose to

[6] The turnover of customer records to the NSA by AT&T and other telecommunication carriers was widely publicized in May and June 2006. *See*, *e.g.*, Leslie Cauley, *NSA has massive database of Americans' phone calls*, USA Today, May 11, 2006, at 1A (available at http://www.usatoday.com/news/washington/2006-05-10-nsa_x.htm); *see also* J. Kirk Wiebe Decl., ¶ 10.

put its intercept equipment at key junction points within the domestic telecommunications network, such as the Folsom Street Facility, thereby giving itself access to purely domestic as well as international communications. Binney Decl., ¶ 8.

Moreover, the Klein and Marcus evidence is supported by more recent evidence that the capacity of NSA's infrastructure far exceeds the capacity necessary for the storage of discrete, targeted communications or even for the storage of the routing information from all electronic communications. In July 2009, the NSA announced that it was building a one-million-square-foot data center in Fort Williams, Utah. Matthew D. Laplante, *Spies like us: NSA to build huge facility in Utah*, Salt Lake Tribune, July 1, 2009 (available at http://www.sltrib.com/ci_12735293). According to some reports, the Utah facility will have a data storage capacity measured in yottabytes (10^{24} bytes or one septillion bytes). Binney Decl., ¶ 11. The capacity of NSA's planned infrastructure is consistent with seizing both the routing information and the contents of all personal electronic communications. Binney Decl., ¶¶ 11-16; Drake Decl., ¶ 9; J. Kirk Wiebe Decl., ¶¶ 9, 12-14.

III. Issues For Decision

1. Has Congress displaced the state secrets privilege in lawsuits in which electronic surveillance is at issue?

2. Have plaintiffs adequately alleged for purposes of section 1806(f) that they are "aggrieved persons"?

IV. Section 1806(f) Displaces The State Secrets Privilege In Lawsuits Alleging Unlawful Electronic Surveillance

The government has invoked the state secrets privilege as a defense to this action, asserting that certain broad categories of evidence are protected by the privilege and that the action should be dismissed. Dkt. #18, #18-2, #18-3. For the reasons explained below, these contentions lack merit. Congress has displaced the state secrets privilege in electronic surveillance cases with the comprehensive statutory procedures of 50 U.S.C. § 1806(f). The displacement of the government's state secrets defense by section 1806(f) is a question of law as to which there is no genuine dispute of material fact, and thus partial summary judgment rejecting the defense should be granted. *See*

Fed. R. Civ. P. 56; *Golinski v. U.S. Office of Personnel Management*, 824 F. Supp. 2d 968, 978 (N.D. Cal. 2012).

A. The State Secrets Privilege

The state secrets privilege is a common-law evidentiary privilege that may be invoked only by the government. *Al-Haramain Islamic Foundation, Inc. v. Bush* ("*Al-Haramain I*"), 507 F.3d 1190, 1196 (9th Cir. 2007). It arises where " 'there is a reasonable danger' that disclosure [of evidence] will 'expose military matters which, in the interest of national security, should not be divulged.' " *Id*. (quoting *United States v. Reynolds*, 345 U.S. 1, 10 (1953)). Like any other evidentiary privilege, ordinarily its only effect is to exclude specific items of evidence that fall within the scope of the privilege. The case then proceeds forward, " 'with no consequences save those resulting from the loss of evidence.' " *Mohamed v. Jeppesen Dataplan, Inc.*, 614 F.3d 1070, 1082 (9th Cir. 2010) (en banc) (quoting *Al-Haramain I*, 507 F.3d at 1204); *see also Al-Haramain I*, 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' "). "The privileged information is excluded and the trial goes on without it." *General Dynamics Corp. v. United States*, __ U.S. __, 131 S.Ct. 1900, 1906 (2011). 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 v. Browner*, 133 F.3d 1159, 1166 (9th Cir. 1998) (emphasis added); *accord*, *Mohamed*, 614 F.3d at 1083.

In *Mohamed*, the Ninth Circuit identified three other "exceptional circumstances" (614 F.3d at 1077) in which state secrets can lead to the dismissal of a lawsuit. The first is where the "very subject matter" of the lawsuit is a state secret. *Mohamed*, 614 F.3d at 1077-78. This is the so-called *Totten* bar, named after *Totten v. United States*, 92 U.S. 105 (1876), which held that spying contracts are unenforceable. *General Dynamics*, 131 S.Ct at 1906.

The second circumstance is where the excluded evidence makes it impossible for the

defendant to prove up a *valid* defense. *Mohamed*, 614 F.3d at 1083 (citing *In re Sealed Case*, 494 F.3d 139, 153 (D.C. Cir. 2007)). This is a high standard for a defendant to meet: "A 'valid defense' . . . is meritorious and not merely plausible and would *require* judgment for the defendant." *In re Sealed Case*, 494 F.3d at 149 (citations omitted, emphasis 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)).

The third of these "rare circumstances" permitting 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 1083, 1088-89.

The Ninth Circuit held in *Mohamed* that dismissals in the second or third circumstances (the "valid-defense" exception and the "unjustifiable-risk" exception) were authorized by *United States v. Reynolds*, 345 U.S. 1, an early state-secrets decision. *Mohamed*, 614 F.3d at 1083. The Supreme Court, however, effectively overruled *Mohamed's* holding on this point in *General Dynamics*. It held that "*Reynolds* was about the admission of evidence. It decided a purely evidentiary dispute by applying evidentiary rules: The privileged information is excluded and the trial goes on without it." *General Dynamics*, 131 S.Ct. at 1906. The Supreme Court held that the *Totten* bar, the valid-defense exception, and the unjustifiable-risk exception were grounded not in *Reynolds* but in its "common-law authority to fashion contractual remedies in Government-contracting disputes." *Id*. at 1906-07. 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 Court need not decide the full extent to which *General Dynamics* has effectively overruled *Mohamed*, or how much, if any, of *Mohamed* still applies in lawsuits like this one not based on a contract or other voluntary secret relationship between the plaintiff and the government. *See Golinski*, 824 F. Supp. 2d at 983-85 (describing procedure for determining whether intervening Supreme Court authority has effectively overruled prior Ninth Circuit precedent). Section 1806(f)

directs the Court to use, not exclude, state secrets evidence to decide the merits of a plaintiff's claims under procedures that protect the secrecy of the evidence.

B. Congress Has Displaced The State Secrets Privilege With Section 1806(f) In Cases Involving Electronic Surveillance

Section 1806(f) displaces the state secrets privilege in electronic surveillance cases by providing secure procedures by which courts can admit and consider national security evidence that the state secrets privilege would otherwise exclude. Section 1806(f) and the state secrets privilege both address the same subject matter: circumstances in which "disclosure [of evidence] or an adversary hearing would harm the national security of the United States." § 1806(f); *see Al-Haramain I*, 507 F.3d at 1196 (state secrets privilege arises where " 'there is a reasonable danger' that disclosure [of evidence] will 'expose military matters which, in the interest of national security, should not be divulged' "). They differ, however, in what they tell courts to do when confronted with national security evidence. If the state secrets privilege applies, the evidence is excluded. In section 1806(f), by contrast, Congress established a procedure enabling civil actions challenging the lawfulness of electronic surveillance to go forward to a decision on the merits while still protecting the interests of national security. "The statute, unlike the common law state secrets privilege, provides a detailed regime to determine whether surveillance 'was lawfully authorized and conducted.' " *Al-Haramain I*, 507 F.3d at 1205 (quoting § 1806(f)). Rather than excluding national security evidence, as would otherwise occur under the state secrets privilege, Congress instead displaced the state secrets privilege and required courts to use all of the relevant national security evidence, reviewed *in camera* and *ex parte*, in deciding the legality of the surveillance.[7]

[7] *See In re National Security Agency Telecommunications Records Litigation* (*Al-Haramain Islamic Foundation, Inc. v. Bush*), 564 F. Supp. 2d 1109, 1124 (N.D. Cal. 2008) (holding that section 1806(f) displaces the state secrets privilege). The question of whether section 1806(f) displaces the state secrets privilege is one of the issues raised in the pending appeal in *Al-Haramain Islamic Foundation v. Obama*, Ninth Cir. Nos. 11-15468, 11-15535 (argued June 1, 2012). This issue has been before the same panel of the Ninth Circuit in three previous appeals (*Al-Haramain I; Hepting v. AT&T; Jewel*), and in each of these appeals, the Ninth Circuit has found it unnecessary to decide the issue. In the pending *Al-Haramain* appeal, the parties have presented grounds that would permit the Ninth Circuit to affirm or reverse without reaching the section 1806(f) issue. In its remand order in this case, the Ninth Circuit, rather than suggesting that this Court should await a

In relevant part, section 1806(f) provides:

> . . . 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 . . . to discover or obtain applications or orders or other *materials relating to electronic surveillance* . . . the United States district court . . . shall, *notwithstanding any other law*, if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States, *review* in camera and ex parte the application, order, and such other *materials relating to the surveillance* as may be necessary *to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted*.

§ 1806(f) (emphasis added).[8]

Congress' purpose in section 1806(f) is what its text states it to be: to provide a method "to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted" in those instances where the government tells the court that "disclosure or an adversary hearing would harm the national security of the United States." § 1806(f). Congress has required the courts to decide the merits of the lawfulness of electronic surveillance by "review[ing] in camera and ex parte the application, order, and such other materials relating to the surveillance as may be necessary." *Id*.

In cases involving electronic surveillance, section 1806(f) displaces and supersedes the state secrets privilege. Congress expressly provided that section 1806(f) applies "notwithstanding any other law," including the state secrets privilege. This expression of Congress' intent to displace the state secrets privilege in cases challenging the lawfulness of electronic surveillance is unequivocal.

There is no doubt that Congress has the power to displace the state secrets privilege: "Congress, of course, has plenary authority over the promulgation of evidentiary rules for the federal courts." *Usery v. Turner Elkhorn Mining Co.*, 428 U.S. 1, 31 (1976). Congress has also set the standard by which the question of displacement should be judged: Federal Rule of Evidence 501 mandates that whenever a "federal statute" "provides otherwise," the common law governing

---

possible ruling in *Al-Haramain* on the section 1806(f) issue, instructed this Court to determine the validity of the government's state secret defense. *Jewel*, 673 F.3d at 913-14.

[8] The full text of section 1806(f) and other pertinent sections of FISA are set forth in the statutory appendix attached hereto.

the state secrets privilege is displaced.[9] Fed. R. Evid. 501; *see* H.R. Rep. No. 93-650 (1973), *reprinted in* 1974 U.S.C.C.A.N. 7075, 7082 (explaining that Rule 501 encompasses the "secrets of state" privilege); S. Rep. No. 93-1277 (1974), *reprinted in* 1974 U.S.C.C.A.N. 7051, 7058 (same). Section 1806(f) meets this test: it is a federal statute that provides for the discovery and admission, under special protective procedures and "notwithstanding any other law" (§ 1806(f)), of evidence the state secrets privilege would otherwise exclude.

Section 1806(f) leaves no room for the state secrets privilege to operate. In electronic surveillance cases, section 1806(f) and the state secrets privilege are mutually exclusive because section 1806(f) directs courts to use national security evidence that the state secrets privilege would otherwise exclude. Applying the state secrets privilege in an electronic surveillance lawsuit would mean nullifying section 1806(f) and preventing courts from adjudicating the legality of electronic surveillance, contrary to Congress' intent.

C. FISA's Statutory Scheme And Legislative History Confirm That Section 1806(f) Displaces The State Secrets Privilege

1. Congress Enacted FISA To Establish Comprehensive Control Over National Security Electronic Surveillance

FISA's statutory scheme and legislative history further reinforce section 1806(f)'s plain language displacing the state secrets privilege. FISA was enacted in 1978 in the wake of the Church Committee's Senate investigation revealing that for many decades the Executive, without any warrants or other lawful authority, had been conducting secret dragnet surveillance invading the privacy and violating the constitutional rights of thousands of ordinary Americans. S. Select Comm. to Study Governmental Operations with Respect to Intelligence Activities, *Book II: Intelligence Activities and the Rights of Americans*, S. Rep. No. 94-755 (1976) (hereafter "Book

[9] Congress itself drafted Rule 501, unlike most provisions of the Federal Rules of Evidence, which were drafted by the advisory committee on the Federal Rules of Evidence. As originally enacted by Congress in 1975, Rule 501 provided that "the privilege of . . . [the] government . . . shall be governed by the principles of the common law" "[e]xcept as otherwise . . . provided by Act of Congress." Pub. L. No. 93-595, § 1, 88 Stat. 1933 (1975), *codified as* Fed. R. Evid. 501. Rule 501 was operative at the time section 1806(f) was enacted in 1978. In December 2011, Rule 501 was reworded, and now states that the common law "governs a claim of privilege unless any of the following provides otherwise: . . . a federal statute." Fed. R. Evid. 501. These changes are "stylistic only." Fed. R. Evid. 501, advisory committee's 2011 note.

II").[10]

The Church Committee concluded that the "massive record of intelligence abuses over the years" had "undermined the constitutional rights of citizens . . . primarily because checks and balances designed by the framers of the Constitution to assure accountability have not been applied." Book II at 290, 289. The Committee urged "fundamental reform," recommending legislation to "make clear to the Executive branch that [Congress] will not condone, and does not accept, any theory of inherent or implied authority to violate the Constitution, the proposed new charters, or any other statutes." *Id*. at 289, 296-97. Citing *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579 (1952), it noted that "there would be no such authority after Congress has . . . *covered the field* by enactment of a comprehensive legislative charter" that would "provide the exclusive legal authority for domestic security activities" and prohibit "warrantless electronic surveillance." Book II at 297 & n.10 (emphasis added).

The Committee recommended the creation of civil remedies for unlawful surveillance. The purpose of these remedies would be both to "afford effective redress to people who are injured by improper federal intelligence activity" and "to deter improper intelligence activity." Book II at 336. The Committee also anticipated section 1806(f)'s displacement of the state secrets privilege to permit civil claims of unlawful surveillance to be litigated, stating that "courts will be able to fashion discovery procedures, including inspections of materials in chambers, and to issue orders as the interests of justice require, to allow plaintiffs with substantial claims to uncover enough factual material to argue their case, while protecting the secrecy of governmental information in which there is a legitimate security interest." *Id*. at 337.

FISA was Congress' response to the Church Committee's recommendations: "This legislation is in large measure a response to the revelations that warrantless electronic surveillance in the name of national security has been seriously abused." S. Rep. No. 95-604(I) at 7 (1977), *reprinted in* 1978 U.S.C.C.A.N. 3904, 3908. FISA implemented the Church Committee's recommendations by imposing strict limits on the Executive's power to conduct electronic

[10] Available at http://www.aarclibrary.org/publib/contents/church/contents_church_reports.htm.

surveillance. *E.g.*, S. Rep. No. 95-604(I), at 8, 1978 U.S.C.C.A.N. at 3910 (FISA "curb[s] the practice by which the Executive Branch may conduct warrantless electronic surveillance on its own unilateral determination that national security justifies it"); S. Rep. No. 94-1035, at 11 (1976) ("the past record establishes clearly that the executive branch cannot be the sole or final arbiter of when such proper circumstances [justifying electronic surveillance] exist"), 20 ("executive self-restraint, in the area of national security electronic surveillance, is neither feasible nor wise"). By providing "effective, reasonable safeguards to ensure accountability and prevent improper surveillance" by the Executive, FISA restored the balance between the protection of civil liberties and the protection of the national security. S. Rep. No. 95-604(I), at 7, 1978 U.S.C.C.A.N. at 3908.

2. Section 1806(f) Is An Essential Element Of Congress' Comprehensive Scheme For Judicially Enforcing The Limitations It Has Imposed On Electronic Surveillance

To ensure that the Executive could not evade the limits Congress imposed on electronic surveillance, Congress expressly provided in FISA that the statutory authorizations of FISA, the Wiretap Act, and the Stored Communications Act (SCA) are the exclusive means by which the Executive may conduct electronic surveillance within the United States:

> [P]rocedures in this chapter [the Wiretap Act, 18 U.S.C. §§ 2510-2522] or chapter 121 [the Stored Communications Act, 18 U.S.C. §§ 2701-2712] and the Foreign Intelligence Surveillance Act of 1978 shall be the *exclusive means* by which electronic surveillance, as defined in section 101 of such Act [50 U.S.C. § 1801], and the interception of domestic wire, oral, and electronic communications may be conducted.

18 U.S.C. § 2511(2)(f) (emphasis added). Congress reconfirmed this exclusivity when it enacted the FISA Amendments Act of 2008. 50 U.S.C. § 1812.

Given the history of past executive abuses, Congress ensured that its mandate of statutory exclusivity would become a reality by establishing mechanisms for judicial enforcement of the comprehensive procedural and substantive limitations on electronic surveillance it had imposed on the Executive. Accordingly, FISA provides for judicial review of national security electronic surveillance *before* it occurs, requiring (with limited exceptions) that the government obtain a warrant from the Foreign Intelligence Surveillance Court ("FISC") before conducting surveillance. *See* 50 U.S.C. § 1804.

FISA also authorizes the courts to review the legality of governmental surveillance *after* it has occurred. It does so by creating criminal and civil liability for unlawful electronic surveillance (50 U.S.C. §§ 1809, 1810) and by providing for the suppression in criminal cases of unlawfully obtained surveillance evidence (50 U.S.C. § 1806(e)). It also does so by creating section 1806(f)'s requirement that courts determine the legality of surveillance and that they do so using national security evidence, instead of excluding that evidence under the state secrets privilege. Both FISA's civil liability provision, section 1810, and section 1806(f)'s mandate for using national security evidence were enacted in 1978 as part of the original FISA statute and have never been amended or cut back. Pub. L. No. 95-511, §§ 106(f), 110; 92 Stat. at 1794, 1796.

Section 1806(f)'s application to civil cases enforcing statutory and constitutional limits on electronic surveillance is a necessary part of Congress' statutory scheme regulating electronic surveillance. Without section 1806(f), the civil enforcement mechanism Congress created to prevent surveillance not authorized by FISA, the Wiretap Act, or the SCA would be toothless. By asserting the state secrets privilege to block judicial review of the lawfulness of its activities, the Executive could free itself from the restraints of FISA, the Wiretap Act, and the SCA and once again "conduct warrantless electronic surveillance on its own unilateral determination that national security justifies it." S. Rep. No. 95-604(I) at 8, 1978 U.S.C.C.A.N. at 3910.

FISA's legislative history confirms that section 1806(f) applies to civil cases in which a plaintiff is seeking a determination of the legality of electronic surveillance in order to vindicate constitutional and statutory rights, as well as to criminal cases in which a defendant is seeking to suppress surveillance evidence:

> The conferees [of the joint House and Senate Committee of Conference] agree that an in camera and ex parte proceeding is appropriate for determining the lawfulness of electronic surveillance *in both criminal and civil cases*.

H.R. Conf. Rep. No. 95-1720, at 32 (1978)*, reprinted in* 1978 U.S.C.C.A.N. 4048, 4061 (emphasis added) (hereafter "FISA Conf. Rep.").

Section 1806(f) applies to all civil claims challenging the lawfulness of electronic surveillance, whether brought under section 1810 of FISA or some other law, such as the constitutional claims, Wiretap Act claims, and SCA claims brought by plaintiffs here. Section

1806(f) requires the court to determine whether the challenged surveillance was "lawfully authorized and conducted" under all applicable legal standards. In addition, section 1806(f) applies to all electronic surveillance, whatever its purpose. FISA defines "electronic surveillance" to include any "acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication . . . without the consent of any party thereto." 50 U.S.C. § 1801(f)(2). This definition of "electronic surveillance" is not limited to foreign intelligence surveillance under FISA but includes any acquisition of a domestic wire communication.

Section 1806(f) also applies to plaintiffs' communications records claims because acquiring those records is electronic surveillance under FISA. "Electronic surveillance" is the acquisition of the "contents" of communications. 50 U.S.C. § 1801(f)(2). The statutory term "contents" encompasses communications records because FISA defines "contents" to include "information concerning the *identity of the parties* to such communication or the *existence* . . . of that communication." 50 U.S.C. § 1801(n) (emphasis added). Independently, information concerning disclosure of communications records is subject to section 1806(f) because such information is "material[] relating to the surveillance." § 1806(f).

FISA's civil remedy provisions and section 1806(f)'s directive thus are both essential elements of FISA's statutory scheme. Section 1806(f) provides the practical means by which the civil liability created to enforce substantive limitations on surveillance and to ensure that only statutorily authorized electronic surveillance occurs can be litigated without endangering the national security.[11]

V. Section 1806(f) Directs This Court To Determine Whether Defendants Subjected Plaintiffs To Unlawful Surveillance

For the reasons explained in the preceding section, section 1806(f) unconditionally displaces any application of the state secrets privilege in this lawsuit, because plaintiffs' claims all allege unlawful electronic surveillance. Moreover, because the government has asserted that

[11] Congress similarly enacted the Classified Information Procedures Act (CIPA), 18 U.S.C. App. 3, to make it possible to litigate criminal cases involving state secrets. CIPA permits courts to use a variety of procedures, including summaries in place of classified evidence, to enable litigation to go forward consistent with due process.

national security evidence exists that is relevant to plaintiffs' claims, and because plaintiffs are "aggrieved persons" who have sought "to discover . . . materials relating to the surveillance" (§ 1806(f)), section 1806(f)'s procedures for handling that evidence under secure procedures have been triggered.

Plaintiffs have rightfully sought discovery of materials relating to electronic surveillance that are relevant to their claims. Dkt. #30. The government has asserted that disclosure of evidence relating to plaintiffs' claims would allegedly harm the national security of the United States. Dkt. #18-3 at 3 ("Disclosure of the information covered by this privilege assertion reasonably could be expected to cause exceptionally grave damage to the national security of the United States."); *accord*, Dkt. #18-4 at 3; *see also* Dkt. #31 at 14 (government's statement that plaintiffs' discovery request (Dkt. #30) "demands discovery of the very facts at issue in the privilege assertion"). Accordingly, section 1806(f) directs the Court to use section 1806(f)'s procedures "to determine whether surveillance 'was lawfully authorized and conducted' " (*Al-Haramain I*, 507 F.3d at 1205 (quoting § 1806(f))).

Plaintiffs are "aggrieved persons." Under FISA, an "aggrieved person" is simply either "a person who is the *target of* an electronic surveillance *or* any other person whose communications or activities were *subject to* electronic surveillance." 50 U.S.C. § 1801(k) (emphasis added). Section 1810's civil remedy is available to any "aggrieved person." Congress' intent in creating the "aggrieved person" standard was to make standing to bring FISA claims "coextensive, but no broader than, those persons who have standing to raise claims under the Fourth Amendment with respect to electronic surveillance." H.R. Rep. No. 95-1283, at 66 (1978). The term was meant to exclude only "persons, not parties to a communication, who may have been mentioned or talked about by others," because "such persons have no fourth amendment privacy right in conversations *about* them." *Id*. (emphasis added). Congress had "no intent to create a statutory right in such persons," and the only purpose of the "aggrieved person" limitation was to exclude from FISA's remedies those who were not parties to the intercepted communication. *Id*.

Section 1806(f) does not require a plaintiff to *prove* he or she is an "aggrieved person" who has been surveilled before it comes into play. In the text of section 1806(f), "aggrieved person" is

merely a description of a person subjected to surveillance who is seeking "to discover . . . materials relating to the surveillance" "pursuant to any . . . statute or rule of the United States." The purpose of discovery for a plaintiff is to obtain evidence needed to prove his or her claims. Under settled law, namely the Federal Rules of Civil Procedure, a plaintiff may propound discovery requests without first proving up the elements of his or her claim. *See* Fed. R. Civ. P. 26(b); *Beck v. Prupis*, 529 U.S. 494, 500-501 (2000) (When Congress uses language with a settled meaning, Congress " 'presumably knows and adopts the cluster of ideas that were attached to each borrowed word in the body of learning from which it was taken and the meaning its use will convey to the judicial mind unless otherwise instructed.' " (quoting *Morissette v. United States*, 342 U.S. 246, 263 (1952))). Section 1806(f) does not limit a plaintiff's right to propound discovery.

Moreover, the plaintiff's discovery request is not, in and of itself, the event that triggers section 1806(f)'s *in camera*, *ex parte* procedures. Rather, the trigger is the government's assertion that national security evidence is at issue. § 1806(f). Without an assertion by the government that national security evidence is at issue, section 1806(f)'s *in camera*, *ex parte* procedures never come into play, discovery and trial continue along their ordinary course, evidence is disclosed, and the district court determines the lawfulness of the surveillance in open proceedings. S. Rep. No. 95-701, at 63 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3973, 4032 ("The special procedures . . . cannot be invoked until they are triggered by a Government affidavit that disclosure or an adversary hearing would harm the national security . . . . If no such assertion is made, the committee envisions . . . mandatory disclosure . . . ."); *see also* FISA Conf. Rep. at 31-32, 1978 U.S.C.C.A.N. at 4060-61. Because it is the government, not the plaintiff, that triggers section 1806(f), the plaintiff does not have to prove anything to trigger its operation.

The government has previously argued that, even if section 1806(f) displaces the state secrets privilege, it does not apply to plaintiffs' claims. It asserts that section 1806(f) applies only if the plaintiff at the pleading stage and before seeking discovery first proves up both standing and a *prima facie* case on the merits, including proving by a preponderance of the evidence that he or she is an "aggrieved person" within the meaning of FISA. This is not the law.

The government makes up its position out of whole cloth. Nothing in FISA requires

plaintiffs to *prove* at the outset that they are aggrieved persons before their lawsuit, and discovery, can go forward. As explained above, the statutory language expressly permits the use of section 1806(f) when a plaintiff seeks discovery. In turn, discovery is proper on matters within the scope of a plaintiff's well-pleaded allegations. *See* Fed. R. Civ. P. 11(b)(3) (factual allegations are well-pleaded if they "will likely have evidentiary support after a reasonable opportunity for further investigation or discovery"); 26(b)(1) (permitting discovery of matters "relevant to any party's claim or defense"). Thus, well-pleaded allegations of electronic surveillance are sufficient to support a discovery request to which section 1806(f) applies. It would turn section 1806(f), and the rules of discovery and trial, upside down to require instead, as the government has suggested, that plaintiffs first prove they have been subjected to surveillance before permitting them to request discovery relating to the surveillance.

As the Ninth Circuit has held, plaintiffs have satisfied their burden of adequately alleging standing for their claims, including alleging that the individual electronic communications of each of them have been intercepted. *Jewel*, 673 F.3d at 910. Moreover, because each plaintiff has alleged that his or her own communications and communications records were intercepted and acquired by defendants, plaintiffs have each alleged not only a concrete and particularized injury but also that they are "aggrieved persons," *i.e.*, "person[s] whose communications or activities were subject to electronic surveillance." 50 U.S.C. § 1801(k). Plaintiffs do not allege surveillance of communications to which they were *not* a party and in which they were only mentioned or talked about—the only type of surveillance excluded from the definition of "aggrieved person."

In addition, plaintiffs have not simply alleged generally that their communications and communications records have been subjected to electronic surveillance. They have presented detailed and extensive allegations of the manner in which the surveillance of their communications and communications records has been conducted. Dkt. #1 at ¶¶ 39-90.

Finally, although only well-pleaded allegations are required at this stage, plaintiffs possess substantial evidence that they are aggrieved persons who have been subjected to unlawful electronic surveillance. For example, the Klein and Marcus declarations and AT&T's documents establish that the NSA has intercepted and duplicated the communications transiting AT&T's

communications facility in San Francisco and elsewhere through which plaintiffs' communications travel. *See generally* Klein Decl.; Marcus Decl.; Russell Decl. That interception was part of the PSP's broader program of unlawful intelligence activities in which the law and the privacy rights of U.S. citizens were violated. Binney Decl., ¶ 5; Drake Decl., ¶ 7. That interception also occurred in the context of NSA infrastructure that far exceeds the capacity necessary for the storage of discrete, targeted communications or even for the storage of the routing information from all electronic communications. Binney Decl., ¶¶ 7-16; Drake Decl., ¶¶ 8-10; J. Kirk Wiebe Decl., ¶¶ 7-14. Thus, even if plaintiffs were required to produce evidence showing that they have been subjected to electronic surveillance in order to demonstrate they are aggrieved persons, they have done so.

VI. Conclusion

Plaintiffs' motion for partial summary judgment should be granted.

DATE: June 29, 2012

Respectfully submitted,

s/ Richard R. Wiebe
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

STATUTORY APPENDIX

50 U.S.C. § 1806(f) - In camera and ex parte review by district court.

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

50 U.S.C. § 1801 - Definitions

As used in this subchapter:

* * * *

(f) "Electronic surveillance" means—

* * * *

(2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States, but does not include the

acquisition of those communications of computer trespassers that would be permissible under section 2511 (2)(i) of title 18;

* * * *

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

* * * *

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

* * * *