Case3:08-cv-04373-JSW Document102 Filed09/12/12 Page1 of 62

1	STUART F. DELERY					
	Acting Assistant Attorney General					
2	JOSEPH H. HUNT					
3	Director, Federal Programs Branch					
	VINCENT M. GARVEY					
4	Deputy Branch Director ANTHONY J. COPPOLINO					
5	Special Litigation Counsel					
	tony.coppolino@usdoj.gov					
6	MARCIA BERMAN					
7	Senior Trial Counsel					
	U.S. Department of Justice					
8	Civil Division, Federal Programs Branch					
	20 Massachusetts Avenue, NW, Rm. 610	2				
9	Washington, D.C. 20001 Phone: (202) 514-4782					
10	Fax: (202) 616-8460					
	Attorneys for the Government Defendants	5				
11	Sued in their Official Capacity	,				
12						
			DISTRICT COURT			
13	NORTHERN DISTRICT OF CALIFORNIA					
14	SAN FR	ANCIS	CO DIVISION			
15	CAROLYN JEWEL, et al.,)	Case No. 3:08-cv-04373-JSW			
16)				
	Plaintiffs,)	GOVERNMENT DEFENDANTS'			
17)	NOTICE OF MOTION AND			
$_{18}$	V.)	MOTION TO DISMISS AND			
10	NATIONAL GEOLOGY A GENOV)	FOR SUMMARY JUDGMENT;			
19	NATIONAL SECURITY AGENCY)	OPPOSITION TO PLAINTIFFS' MOTION FOR PARTIAL			
, α	et al.,)	SUMMARY JUDGMENT			
20	Defendants.)	SUMMANT SUDGMENT			
21	2 515113411131)	Date: November 2, 2012			
22)	Time: 9:00 a.m.			
22)	Courtroom: $11 - 19^{th}$ Floor			
23)	Judge Jeffrey S. White			
24						
25						
26						
27						
28						
	I and the second					

Government Defendants' Notice of Second Motion to Dismiss and For Summary Judgment; Opposition to Plaintiffs' Motion for Partial Summary Judgment *Jewel v. National Security Agency* (08-cv-4373-JSW)

9 10

11 12

13

14 15

16

17

18

19 20

21

22 23

24 25

26 27

28

NOTICE OF MOTION

PLEASE TAKE NOTICE that, on November 2, 2012 at 9:00 a.m, before Judge Jeffrey S. White, Defendants NATIONAL SECURITY AGENCY; KEITH B. ALEXANDER, Director of the NSA, in his official capacity; the UNITED STATES OF AMERICA; BARACK OBAMA, President of the United States, in his official capacity; DEPARTMENT OF JUSTICE; ERIC HOLDER, the Attorney General, in his official capacity; and JAMES R. CLAPPER, Director of National Intelligence, in his official capacity (hereafter the "Government Defendants") will move to dismiss the claims in the Complaint pursuant to Rule 12(b)(1) of the Federal Rules of Civil Procedure and will also seek summary judgment as to all claims against all defendants pursuant to Rule 56 of the Federal Rules of Civil Procedure. The grounds for this motion are as follows:

- 1. The Court lacks subject matter jurisdiction with respect to plaintiffs' statutory claims against the Government Defendants sued because Congress has not waived sovereign immunity as to these claims and the relief sought is not otherwise available as a matter of law against the Government Defendants.
- 2. Plaintiffs' claims against all defendants (including the individual capacity defendants) should be dismissed on the ground that litigation of plaintiffs' claims would risk or require the disclosure of certain information that is properly protected by statutory protections and the state secrets privilege asserted in this action by the Director of National Intelligence and by the National Security Agency.

The grounds for this motion are set forth in the accompanying (i) Memorandum of Points and Authorities in Support of the Government Defendants' Motion to Dismiss and for Summary Judgment; Opposition to Plaintiffs' Motion for Partial Summary Judgment; (ii) Public Declaration of James R. Clapper, Director of National Intelligence (hereafter "Public DNI Decl."); (iii) Public Declaration of Frances Fleisch, National Security Agency (hereafter "Public

Case3:08-cv-04373-JSW Document102 Filed09/12/12 Page3 of 62

1	NSA Decl."). Additional ground	ds for these motions are also set forth in the (iv) Classified State			
2	Secrets Privilege Declaration of James R. Clapper, Director of National Intelligence; and the (v)				
3	Classified Declaration of Frances Fleisch, National Security Agency. These classified materials				
4	have been lodged with the court security officer and are available upon request solely for the				
5	Court's in camera, ex parte revi	ew.			
6	September 12, 2012	Respectfully Submitted,			
7		•			
8		STUART F. DELERY Acting Assistant Attorney General			
9		JOSEPH H. HUNT			
10		Director, Federal Programs Branch			
11		VINCENT M. GARVEY			
12		Deputy Branch Director			
13		s/ Anthony J. Coppolino			
14		ANTHONY J. COPPOLINO Special Litigation Counsel			
15		tony.coppolino@usdoj.gov			
16		s/ Marcia Berman			
17		MARCIA BERMAN Senior Trial Counsel			
		Sellioi IIIai Coulisei			
18		U.S. Department of Justice			
19		Civil Division, Federal Programs Branch 20 Massachusetts Avenue, NW, Rm. 6102			
20		Washington, D.C. 20001			
21		Phone: (202) 514-4782 Fax: (202) 616-8460			
22					
23		Attorneys for the Government Defendants Sued in their Official Capacities			
		·			
24					
25					
26					
27					
28					

Case3:08-cv-04373-JSW Document102 Filed09/12/12 Page4 of 62

1	STUART F. DELERY			
2	Acting Assistant Attorney General JOSEPH H. HUNT			
3	Director, Federal Programs Branch			
3	VINCENT M. GARVEY			
4	Deputy Branch Director ANTHONY J. COPPOLINO			
5	Special Litigation Counsel			
6	tony.coppolino@usdoj.gov MARCIA BERMAN			
	Senior Trial Counsel			
7	U.S. Department of Justice			
8	Civil Division, Federal Programs Branch 20 Massachusetts Avenue, NW, Rm. 6102			
9	Washington, D.C. 20001			
10	Phone: (202) 514-4782			
	Fax: (202) 616-8460 Attorneys for the Government Defendants			
11	Sued in their Official Capacity			
12	LINITED STATES	DISTRICT COURT		
13	NORTHERN DISTRICT OF CALIFORNIA			
$_{14}$	SAN FRANCISCO DIVISION			
15)			
	CAROLYN JEWEL, et al.,	Case No. 3:08-cv-04373-JSW		
16	Plaintiffs,	MEMORANDUM IN SUPPORT		
17)	OF GOVERNMENT DEFENDANTS'		
18	v.)	MOTION TO DISMISS AND FOR SUMMARY JUDGMENT;		
19	NATIONAL SECURITY AGENCY, et al.)	OPPOSITION TO PLAINTIFFS'		
		MOTION FOR PARTIAL		
20				
	Defendants.)	SUMMARY JUDGMENT		
21))	Date: November 2, 2012		
	Defendants.	Date: November 2, 2012 Time: 9:00 a.m.		
22))))))	Date: November 2, 2012		
22 23))))))	Date: November 2, 2012 Time: 9:00 a.m. Courtroom: 11 – 19 th Floor		
22 23))))))	Date: November 2, 2012 Time: 9:00 a.m. Courtroom: 11 – 19 th Floor		
22 23 24)))))	Date: November 2, 2012 Time: 9:00 a.m. Courtroom: 11 – 19 th Floor		
21 22 23 24 25 26	Defendants.)))))	Date: November 2, 2012 Time: 9:00 a.m. Courtroom: 11 – 19 th Floor		
22 23 24 25 26))))))	Date: November 2, 2012 Time: 9:00 a.m. Courtroom: 11 – 19 th Floor		
22 23 24 25))))))	Date: November 2, 2012 Time: 9:00 a.m. Courtroom: 11 – 19 th Floor		

Government Defendants' Notice of Second Motion to Dismiss and For Summary Judgment; Opposition to Plaintiffs' Motion for Partial Summary Judgment *Jewel v. National Security Agency* (08-cv-4373-JSW)

Case3:08-cv-04373-JSW Document102 Filed09/12/12 Page5 of 62

TABLE OF CONTENTS 1 2 BACKGROUND3 3 ARGUMENT5 4 Congress Has Not Waived Sovereign Immunity For Plaintiffs' Statutory Claims I. 5 Congress Has Not Waived Sovereign Immunity For Plaintiffs' Statutory Claims II. 6 7 A. 9 2. The Court's Independent Evaluation of the Privilege 10 11 3. 12 Plaintiffs' Allegations of Dragnet Surveillance Program В. 13 Cannot Be Litigated Without Information Over Which The United States 14 IV. Plaintiffs' Motion For Partial Summary Judgment Should Be 15 Denied Because Litigation Of Plaintiffs' Claims May Not Proceed 16 Congress May Not Displace the Common Law Without a Α. 17 18 Congress' "Comprehensive" Regulation Of Foreign Intelligence В. Surveillance Does Not Displace The State 19 20 The Text of Subsection 1806(f) Does Not Displace the State Secrets C. Privilege or Permit Discovery Into Whether A Person Has Been Subject to 21 22 Legislative History Supports the Conclusion that D. Subsection 1806(f) Does Not Displace the State Secrets Privilege or 23 Permit Discovery Into Whether Alleged Surveillance Has Occurred. 38 24 Judicial Authority Supports the Conclusion that Subsection 1806(f) Does E. Not Displace the State Secrets Privilege 25 or Permit Discovery Into Whether Alleged Surveillance Has Occurred. 42 26 F. Application of Subsection 1806(f) in this Case Would Itself Risk 27 28

Government Defendants' Notice of Second Motion to Dismiss and For Summary Judgment; Opposition to Plaintiffs' Motion for Partial Summary Judgment *Jewel v. National Security Agency* (08-cv-4373-JSW)

Case3:08-cv-04373-JSW Document102 Filed09/12/12 Page6 of 62 IV.

Case3:08-cv-04373-JSW Document102 Filed09/12/12 Page7 of 62

TABLE OF AUTHORITIES Federal Cases ACLU Foundation v. Barr, ACLU v. NSA, Adam v. Norton. Adams v. United States, Alderman v. United States, Al-Haramain Islamic Foundation, Inc. v. Obama, Al-Haramain Islamic Foundation, Inc. v. Bush, American Elec. Power Co. v. Connecticut, Aminoil U.S.A., Inc. v. Cal. State Water Ctrl. Bd., Armstrong v. Bush, Astoria Fed. Sav. & Loan Ass'n v. Solimino. Bacon v. United States,

Government Defendants' Notice of Second Motion to Dismiss and For Summary Judgment; Opposition to Plaintiffs' Motion for Partial Summary Judgment *Jewel v. National Security Agency* (08-cv-4373-JSW)

Case3:08-cv-04373-JSW Document102 Filed09/12/12 Page8 of 62 Block v. North Dakota ex rel. Bd. of University and School Lands, Cent. Bank of Denver v. First Interstate Bank of Denver, Cent. Res. Life of North America Ins. Co. v. Struve, Chamber of Commerce v. Reich, Children's Hosp. Health Ctr. v. Belshe, City of Los Angeles v. Lyons, City of Milwaukee v. Illinois, County of Oneida v. Oneida Indian Nation, Davis v. Michigan Dep't of Treasury, Department of the Navy v. Egan, Dep't of the Army v. Blue Fox, Inc., Dugan v. Rank, E.E.O.C. v. Peabody Western Coal Co., Ellsberg v. Mitchell,

Government Defendants' Notice of Second Motion to Dismiss and For Summary Judgment; Opposition to Plaintiffs' Motion for Partial Summary Judgment *Jewel v. National Security Agency* (08-cv-4373-JSW)

Case3:08-cv-04373-JSW Document102 Filed09/12/12 Page9 of 62 El-Masri v. United States, FAA v. Cooper, Farnsworth Cannon, Inc. v. Grimes, FDIC v. Meyer, Fitzgerald v. Penthouse Int'l, Ltd., Franklin v. Massachusetts, Freeman v. DirecTV, Inc., Gelbard v. United States, General Dynamics Corp. v. United States, Geyen v. Marsh, Hawaii v. Gordon, Hepting v. AT&T Corp., In re Grand Jury Investigation (Doe), In re Grand Jury Witness (Whitnack), Government Defendants' Notice of Second Motion to Dismiss and For Summary Judgment; Opposition to Plaintiffs' Motion for Partial Summary Judgment Jewel v. National Security Agency (08-cv-4373-JSW)

Case3:08-cv-04373-JSW Document102 Filed09/12/12 Page10 of 62 *In re Hanford Nuclear Reservation Litigation*, 1 2 In re National Security Agency Telecommunications Records Litigation (Al-Haramain Islamic 3 Foundation, Inc. v. Bush), 4 5 In re National Security Agency Telecommunications Records Litigation, 6 7 8 In re National Security Agency Telecommunications Records Litigation (Al-Haramain Islamic 9 Foundation, Inc. v. Obama), 10 11 In re Niles, 12 In re Sealed Case, 13 14 15 Jewel v. National Security Agency, 16 17 Jewel v. National Security Agency, 18 Kasza v. Browner, 19 20 21 Larson v. Domestic & Foreign Commerce Corp., 22 23 Lewis v. Casey, 24 25 Lujan v. Defenders of Wildlife, 26 27 Mobil Oil Corp. v. Higginbotham, 28 Government Defendants' Notice of Second Motion to Dismiss and For Summary Judgment; Opposition to Plaintiffs' Motion for Partial Summary Judgment Jewel v. National Security Agency (08-cv-4373-JSW)

Case3:08-cv-04373-JSW Document102 Filed09/12/12 Page11 of 62 Mohamed v. Jeppesen Dataplan, Inc., New Jersey v. T.L.O., Norfolk Redevelopment & Housing Auth. v. Chesapeake & Potomac Tel. Co., O'Connor v. Ortega, Palomar Pomerado Health Sys. v. Belshe, Pennhurst State School & Hosp. v. Halderman, Presbyterian Church (U.S.A.) v. United States, Prescott v. United States, Rakus v. Illinois, Schnapper v. Foley,

Sea-Land Serv., Inc. v. Brown,

Smith v. Maryland,

Sterling v. Tenet,

Tenet v. Doe,

Government Defendants' Notice of Second Motion to Dismiss and For Summary Judgment; Opposition to Plaintiffs' Motion for Partial Summary Judgment Jewel v. National Security Agency (08-cv-4373-JSW)

Vii

Case3:08-cv-04373-JSW Document102 Filed09/12/12 Page12 of 62 Terkel v. AT&T Corp., Totten v. United States, United States Nat'l Bank of Oregon v. Indep. Ins. Agents of Am., Inc., United States v. Abu-Jihaad, United States v. Alter, United States v. Damrah, United States v. Duggan, United States v. Forrester, United States v. Hamide, United States v. Johnson, United States v. Mitchell, United States v. Nixon, United States v. Ott. United States v. Reynolds, Government Defendants' Notice of Second Motion to Dismiss and For Summary Judgment; Opposition to

Plaintiffs' Motion for Partial Summary Judgment Jewel v. National Security Agency (08-cv-4373-JSW)

Case3:08-cv-04373-JSW Document102 Filed09/12/12 Page13 of 62 United States v. Texas, United States v. Warsame, Warth v. Selden, Washington Dep't of Soc. & Health Servs. v. Estate of Keffeler, Weinberger v. Catholic Action of Hawaii/Peace Education Project, **Federal Statutes** 18 U.S.C. § 2703....... 5, 8, 10, 26 18 U.S.C. § 2707.......9 50 U.S.C. § 1810......passim

Case3:08-cv-04373-JSW Document102 Filed09/12/12 Page14 of 62 **United States Constitution Federal Rules**

INTRODUCTION

Plaintiffs in this action allege that, following the 9/11 attacks, then-President George W. Bush authorized the National Security Agency (NSA) to undertake indiscriminate warrantless surveillance of domestic communications with the assistance of major telecommunications companies, and that this alleged "dragnet" surveillance encompassed both the collection of the content of telephone and Internet communications as well the communication records of millions of Americans. *See* Complaint ¶ 1, 7; *see also id.* ¶¶ 9-11; 73-75; 82-97. Plaintiffs claim that the alleged warrantless surveillance violates the First and Fourth Amendments of the United States Constitution, and the separation of powers doctrine, as well as various statutory provisions. Plaintiffs also claim the alleged warrantless surveillance authorized by the President after 9/11 remains ongoing today, and they seek prospective declaratory and injunctive relief to halt such alleged surveillance, as well as damages against the United States and numerous former government officials.

In April 2009, the Director of National Intelligence ("DNI"), supported by the NSA, asserted the state secrets privilege and related statutory protections in this action in order to protect against the disclosure of highly sensitive intelligence sources and methods, and the Government sought dismissal on that basis. However, in 2010, the district court dismissed the case on grounds not advanced by the Government—that plaintiffs had failed to sufficiently allege a personal injury in their complaint—and did not consider the Government's state secrets privilege assertion. *See Jewel v. National Security Agency*, 2010 WL 235075 (N.D. Cal. 2010). The Ninth Circuit reversed and remanded this case in 2011 with instructions that the Court now consider, among other claims and defenses, whether "the government's assertion that the state secrets privilege bars this litigation." *See Jewel v. National Security Agency*, 673 F.3d 902, 913-14 (9th Cir. 2011). Accordingly, the DNI and NSA have renewed the Government's privilege

Case3:08-cv-04373-JSW Document102 Filed09/12/12 Page16 of 62

assertion in this case and again demonstrate why the disclosure of sensitive intelligence sources and methods at issue in this case reasonably could be expected to cause exceptionally grave harm to national security and why, as a result, this action should be dismissed. The Government's privilege assertion has been reviewed and approved pursuant to the Attorney General's 2009 policy concerning the defense of state secrets privilege assertions by the Department of Justice. *See infra*.

The information over which the DNI has asserted privilege is not at the periphery of this case. The very purpose of this litigation is to put at issue whether the NSA undertook certain alleged activities under presidential authorization after 9/11, and whether those activities continue today. At every stage, from standing to the merits, highly classified and properly privileged intelligence sources and methods are at risk of disclosure. The law is clear, however, that where litigation risks or requires the disclosure of information that reasonably could be expected to harm national security, dismissal is required. *Mohamed v. Jeppesen Dataplan, Inc.*, 614 F.3d 1070, 1079 (9th Cir. 2010).

Plaintiffs' principle defense to the privilege assertion is that provisions of the Foreign Intelligence Surveillance Act (FISA) have "displaced" the privilege and establish a framework for litigation of their claims on the merits. In July 2012, plaintiffs filed a motion for partial summary judgment on this basis. Plaintiffs' contention is meritless and their motion should be denied. The FISA procedures cited by plaintiffs are directed at a different circumstance—the use of surveillance evidence in a proceeding against an "aggrieved person"—and do not permit a person merely alleging he or she was subject to surveillance to seek discovery into whether

Government Defendants' Notice of Second Motion to Dismiss and For Summary Judgment; Opposition to Plaintiffs' Motion for Partial Summary Judgment *Jewel v. National Security Agency* (08-cv-4373-JSW)

¹ See Plaintiffs' Motion for Partial Summary Judgment Rejecting the Government Defendants' State Secret Defense (Dkt. 83) (hereafter "Pls. Mem.").

Case3:08-cv-04373-JSW Document102 Filed09/12/12 Page17 of 62

surveillance has occurred.

Before reaching the state secrets privilege question, the Court should narrow the claims for which consideration of the privilege assertion would be necessary by dismissing plaintiffs' statutory claims against the United States and official capacity defendants on the ground that the statutory causes of action at issue do not unambiguously waive sovereign immunity for the specific claims raised against the Government.

BACKGROUND

In December 2005, in response to media reports, then-President Bush acknowledged the existence of a program he authorized after the 9/11 attacks under which the NSA intercepted certain international communications to or from the United States reasonably believed to involve a member or agent of al Qaeda—later referred to as the "Terrorist Surveillance Program" ("TSP"). See In re National Security Agency Telecommunications Records Litigation, 671 F.3d 881, 891 (9th Cir. 2011) (cert. petition pending). Other allegations arose at the time that the NSA had engaged in broader surveillance activities under presidential authorization, including the collection of communication records. See id.

Starting in early 2006, numerous lawsuits were filed across the United States challenging these alleged activities, primarily against telecommunications carriers alleged to have assisted the Government, but also including some lawsuits against Government agencies and officials. In this district, the first case filed was *Hepting v. AT&T* (06-cv-00673-VRW)—a lawsuit against AT&T alleging that it had assisted the Government in alleged intelligence activities. Thereafter, over forty other class action suits against other telecommunications carriers and Government agencies and officials were transferred to this district by the Judicial Panel on Multidistrict Litigation (JPML) and assigned to former Chief Judge Walker under docket number M:06-cv-1791-VRW. *See In re NSA*, 671 F.3d at 891.

In July 2008, Congress enacted the Foreign Intelligence Surveillance Act Amendments Act of 2008 ("FAA") which, *inter alia*, foreclosed a cause of action against telecommunications carriers alleged to have assisted the United States Intelligence Community. *See* Pub.L. No. 110-

Case3:08-cv-04373-JSW Document102 Filed09/12/12 Page18 of 62

1

2

3

4

5

6

7

8

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

261, 122 Stat. 2435, codified at 50 U.S.C. §1885a. Shortly thereafter, the same plaintiffs who had filed the *Hepting* action filed the instant *Jewel* action, which raised identical factual allegations of alleged warrantless surveillance activities but, in this instance, raised claims solely against U.S. Government agencies and officials in both their official and personal capacities.²

In prior proceedings, Judge Walker did not consider the Government's state secrets privilege assertion but, as noted, dismissed this action (and another action pending in MDL 1791 that raised similar allegations—Shubert v. Obama (07-cv-00693)) for lack of standing on the ground that plaintiffs had failed to sufficiently allege a personal injury. See Dkt. 57; 2010 WL 235075 (N.D. Cal. 2010). The Ninth Circuit reversed and remanded both cases in a consolidated order. See Jewel, 673 F.2d at 913-14. The Ninth Circuit found that the Jewel plaintiffs had alleged a sufficient injury in the complaint to satisfy Article III standing requirements at the pleading stage, but did not find that plaintiffs had established their standing as a factual matter. See id. at 908-912. The Court of Appeals noted that the Sixth Circuit, in ACLU v. NSA, 493 F.3d 644, 648 (6th Cir. 2007), held that the state secrets privilege had foreclosed plaintiffs in that case from proving their standing and observed that the plaintiffs here "may face similar procedural, evidentiary and substantive barriers as the plaintiffs in ACLU." Jewel, 673 F.3d at 912. Accordingly, the DNI and NSA now renew their privilege assertion and again demonstrate why properly privileged information is inherently at risk of disclosure, why that privilege assertion forecloses plaintiffs from establishing standing or litigating their claims on the merits, and why as a result this action should be dismissed.

² Lawsuits against telecommunication carriers, including *Hepting*, were subsequently dismissed pursuant to the FAA and that dismissal was upheld by the Ninth Circuit. *See In re NSA*, 671 F.3d 881 (9th Cir. 2011).

ARGUMENT

I.	CONGRESS HAS NOT WAIVED SOVEREIGN IMMUNITY FOR
	PLAINTIFFS' STATUTORY CLAIMS FOR DAMAGES.

Before reaching the state secrets privilege issues, the Court should first narrow the scope of this case by dismissing plaintiffs' statutory claims for money damages against the Government Defendants sued in their official capacity, whether under FISA, 50 U.S.C. §§ 1809, 1810, the Wiretap Act, Electronic Communications Privacy Act ("ECPA"), or the Stored Communications Act ("SCA"). *See* 18 U.S.C. § 2511(1)(a), (1)(c), (1)(d); § 2703(a), (b) and (c). All of these claims fail for the threshold reason that Congress has not waived sovereign immunity for these claims. "'Sovereign immunity is a limitation on the district court's subject matter jurisdiction." *Al-Haramain Islamic Foundation, Inc. v. Obama*, --F.3d --, 2012 WL 3186088, at * 3 n. 2 (9th Cir. Aug. 7, 2012) (quoting *Adam v. Norton*, 636 F.3d 1190, 1192 n. 2 (9th Cir. 2011)).

"Absent a waiver, sovereign immunity shields the Federal Government and its agencies from suit." *Dep't of the Army v. Blue Fox, Inc.*, 525 U.S. 255, 260 (1999) (quoting *FDIC v. Meyer*, 510 U.S. 471, 475 (1994)). Plaintiffs bear the burden of establishing such a waiver. *See Prescott v. United States*, 973 F.2d 696, 701 (9th Cir. 1992).

In sum, plaintiffs' FISA damages claims cannot proceed against the United States under § 1810. Nor do plaintiffs' claims that the government unlawfully surveilled them fit within the specific claims for which Congress waived sovereign immunity in 18 U.S.C. § 2712, which all involve the use and disclosure of information. Section 2712 permits actions against the United States to recover money damages for willful violations of sections 1806(a), 1825(a), and 1845(a) of FISA, and of the Wiretap Act and the ECPA. All three FISA provisions relate to the use and

Case3:08-cv-04373-JSW Document102 Filed09/12/12 Page20 of 62

disclosure of information obtained under FISA, not the mere collection of it.³ As the Ninth Circuit recognized in *Al-Haramain*, "[u]nder this scheme, Al-Haramain can bring a suit for damages against the United States for *use* of the collected information, but cannot bring suit against the government for collection of the information itself." 2012 WL 3186088, at * 5 (emphasis in original).

"A waiver of sovereign immunity cannot be implied but must be unequivocally expressed." *Al-Haramain*, 2012 WL 3186088, at * 3 (quoting *United States v. Mitchell*, 445 U.S. 535, 538 (1980)). Any ambiguity is construed in favor of immunity, and "[a]mbiguity exists if there is a plausible interpretation of the statute that would not authorize money damages against the Government." *FAA v. Cooper*, 132 S. Ct. 1441, 1448 (2012). Any ambiguity in the scope of a waiver of sovereign immunity is likewise construed in favor of immunity: the scope of Congress' waiver must "be clearly discernible from the statutory text in light of traditional interpretive tools. If it is not, then we take the interpretation most favorable to the Government." *Al-Haramain*, 2012 WL 3186088, at * 3 (quoting *Cooper*, 132 S. Ct. at 1448). Plaintiffs rely on 50 U.S.C. § 1810 as their purported source of a waiver of sovereign immunity

³ Subsection 1806(a) provides that "[i]nformation acquired from an electronic surveillance conducted pursuant to this subchapter concerning any United States person may be used and disclosed by Federal officers and employees without the consent of the United States person only in accordance with the minimization procedures required by this subchapter. . . . No information acquired from an electronic surveillance pursuant to this subchapter may be used or disclosed by Federal officers or employees except for lawful purposes." Similarly, subsection 1825(a) provides that "[i]nformation acquired from a physical search conducted pursuant to this subchapter concerning any United States person may be used and disclosed by Federal officers and employees without the consent of the United States person only in accordance with the minimization procedures required by this subchapter. No information acquired from a physical search pursuant to this subchapter may be used or disclosed by Federal officers or employees except for lawful purposes." And subsection 1845(a) provides as well that "[i]nformation acquired from the use of a pen register or trap and trace device installed pursuant to this subchapter concerning any United States person may be used and disclosed by Federal officers and employees without the consent of the United States person only in accordance with the provisions of this section. . . . No information acquired from a pen register or trap and trace device installed and used pursuant to this subchapter may be used or disclosed by Federal officers or employees except for lawful purposes."

Case3:08-cv-04373-JSW Document102 Filed09/12/12 Page21 of 62

for their FISA damages claim. Complaint at ¶ 167. The Ninth Circuit recently squarely rejected this claim in Al-Haramain when it held that § 1810 does not waive sovereign immunity. Hewing to the Supreme Court's command that a waiver of sovereign immunity must be explicit and may not be implied, the Ninth Circuit observed that the statutory definition of "person" did not include the United States. 2012 WL 3186088, at * 4. The court further contrasted the absence of an explicit waiver of sovereign immunity in § 1810 with the presence of one in 18 U.S.C.§ 2712, where Congress located an explicit waiver with respect to certain sections of FISA as part of the USA Patriot Act. *Id.* at * 4-5. Section 2712 provides for civil actions against the United States to recover money damages for certain willful violations of FISA, the Wiretap Act, and the Electronic Communications Privacy Act (ECPA), and sets out detailed procedures that must be followed to file a claim against the United States. The court reasoned that "[i]t would be anomalous to the point of absurdity for Congress, on one hand, to carefully and explicitly waive sovereign immunity with respect to certain FISA sections, set out detailed procedures for suits pursuant to that waiver, and then on the other, cavalierly imply a sovereign immunity waiver with respect to § 1810 by rendering liable any 'person.'" *Id.* at * 6. Finally, the court noted that the predicate for liability under § 1810 is a violation of § 1809, which is a criminal offense. Finding that a government employee in his official capacity (i.e., the United States) could be liable under § 1810 would mean finding that a criminal prosecution could be maintained against an office, rather than an individual, under § 1809, and this would be "unprecedented." Id. at * $7.^{5}$

25

26

27

28

1

2

3

4

5

6

9

10

11

12

13

14

15

16

17

18

19

20

21

22

²⁴

⁴ Section 1810 states: "An aggrieved person, . . . who has been subjected to an electronic surveillance or about whom information obtained by electronic surveillance of such person has been disclosed or used in violation of section 1809 of this title shall have a cause of action against any person who committed such violation"

⁵ For this reason, plaintiffs' counts against the Government for violating 50 U.S.C. § 1809 cannot survive. *See* Complaint at Counts V, VI.

Case3:08-cv-04373-JSW Document102 Filed09/12/12 Page22 of 62

1

2

3

4

5

6

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

The Ninth Circuit's ruling in Al-Haramain is supported by a holistic look at the section of the Patriot Act in which 18 U.S.C.§ 2712 was enacted. See United States Nat'l Bank of Oregon v. Indep. Ins. Agents of Am., Inc., 508 U.S. 439, 455 (1993). In the very same section in which Congress added § 2712 (§ 223 of the Act), it expressly barred suits against the United States for damages and equitable relief based on alleged violations of the Wiretap Act and the ECPA, in both cases by permitting relief only against a person or entity "other than the United States." Section 223(a)(1), (b)(1) of the Patriot Act of 2001, Pub. L. No. 107-56, 115 Stat. 272.⁶ 18 U.S.C. §§ 2520(a), 2707(a). Congress added back liability for willful violations of these two acts and for violations of the three use-and-disclosure provisions of FISA in § 2712 (§ 223(c)(1)). And Congress added the following two similar provisions focused on use and disclosure: (1) "Any willful disclosure or use by an investigative or law enforcement officer or governmental entity of information beyond the extent permitted by [the Wiretap Act] is a violation" of that Act, § 223(a)(3) (codified at 18 U.S.C. 2520(g)); and (2) "Any willful disclosure of a 'record' . . . obtained by an investigative or law enforcement officer, or a governmental entity, pursuant to section 2703 of this title . . . that is not a disclosure made in the proper performance of the official functions of the officer or governmental entity making the disclosure, is a violation of [ECPA]." Section 223(b)(3) (codified at 18 U.S.C. 2707(g)). Not surprisingly, § 223 was titled "Civil Liability for Certain Unauthorized Disclosures." Reading § 223 as a whole, the waiver of sovereign immunity in 18 U.S.C. § 2712 is limited to use-and-disclosure claims, not collection claims, as the Ninth Circuit recognized.

The legislative history of § 223 shows that Congress was indeed focused on the disclosure of information obtained from electronic surveillance, not its collection. Section 223

⁶ Section 223 of the Patriot Act is submitted herewith as Ex. 1.

Case3:08-cv-04373-JSW Document102 Filed09/12/12 Page23 of 62

was an amendment proposed by Representative Barney Frank during the consideration of the Patriot Act before the House Committee on the Judiciary. Citing the historical example of leaks by former FBI Director J. Edgar Hoover of information obtained through surveillance about Dr. Martin Luther King, Jr.'s personal life, Representative Frank explained that an individual subjected to such "inappropriate release of information garnered by surveillance" should have the right to "get damages from the Federal Government." He elaborated as follows: "We have got to build into this a bureaucratic departmental incentive to crack down on this kind of leaking, and I think if we are able to ensure people that we have done the maximum to prevent the inappropriate disclosure of this information, there is less concern about [it] being gathered." Administration's Draft Anti-Terrorism Act of 2001: Hearing Before the H. Comm. on the Judiciary, 107th Cong., 1st Sess., at 17 (2001) (attached as Ex. 2).

In approving Representative Frank's amendment, the House Judiciary Committee described it as providing "increased civil liability for unlawful disclosures of information" obtained by electronic surveillance. *See* H.R. Rep. No. 107-236 (Part I), at 42 (2001) (attached as Ex. 3). Four years later, when Congress reauthorized 18 U.S.C. § 2712 and other provisions of the Patriot Act, it recognized that § 2712 "[i]ncreases civil liability for unauthorized disclosure of pen trap, wiretap, stored communications or FISA information." H.R. Rep. No. 109-174 (Part I), at 496 (2005) (attached as Ex. 4).

Plaintiffs allege that the Government unlawfully collected their communications and communications records, not that the Government used or disclosed any information obtained about them in the manner targeted by the Frank Amendment. Accordingly, § 2712 does not provide a waiver of sovereign immunity for their statutory damages claims.⁷

Government Defendants' Notice of Second Motion to Dismiss and For Summary Judgment; Opposition to Plaintiffs' Motion for Partial Summary Judgment *Jewel v. National Security Agency* (08-cv-4373-JSW)

 $^{^{7}\,}$ Plaintiffs allege that telecommunication carriers, working in concert with NSA, disclosed acquired (cont'd)

II. CONGRESS HAS NOT WAIVED SOVEREIGN IMMUNITY FOR PLAINTIFFS' STATUTORY CLAIMS FOR EQUITABLE RELIEF.

Plaintiffs' statutory claims for declaratory and injunctive relief, presented in Counts V (under FISA, 50 U.S.C. § 1809), VII (under the Wiretap Act, 18 U.S.C. § 2511), X (under the ECPA, 18 U.S.C. § 2703(a), (b)), XIII (under the ECPA, 18 U.S.C. § 2703(c)), and XVI (under the Administrative Procedures Act ("APA"), 5 U.S.C. § 701 *et seq.*), likewise cannot survive because Congress has not waived the Government's sovereign immunity for them.

As noted above, the waiver of sovereign immunity under FISA is contained in 18 U.S.C. § 2712, but this waiver is only for certain claims and remedies. It waives sovereign immunity only for money damages, not equitable relief, and is the "exclusive remedy" against the United States for claims under this section. § 2712(a), (d). Congress provided for equitable relief under the Wiretap Act and the ECPA, but only as to equitable relief running against a "person or entity, other than the United States." 18 U.S.C. §§ 2520(a), 2707(a). Thus, neither FISA, nor the Wiretap Act, nor the ECPA waives sovereign immunity for equitable relief.

Section 702 of the APA does not waive sovereign immunity for the claims at issue here. Although it waives equitable relief for other claims, it contains a significant exception to that waiver which squarely applies. Section 702 provides, "Nothing herein (1) affects other limitations on judicial review . . . or (2) confers authority to grant relief if any other statute that grants consent to suit expressly or impliedly forbids the relief which is sought." This provision

information to the Government, not that the Government disclosed the information. See Complaint at ¶ 9-10, 13, 69-70, 73-84, 90-97. Moreover, nothing in the statutes upon which plaintiffs base their claims creates liability against the United States for allegations of aiding and abetting disclosures by third parties, and the Supreme Court has refused to impose such secondary civil liability absent "congressional direction to do so." Cent. Bank of Denver v. First Interstate Bank of Denver, 511 U.S. 164, 183 (1994); see also id. at 177 ("If . . . Congress intended to impose aiding and abetting liability, we presume it would have used the words 'aid' and 'abet' in the statutory text."). The Ninth Circuit has followed Central Bank of Denver by refusing to find a private cause of action under 18 U.S.C. § 2702 against those who allegedly aid and abet, or conspire with, electronic communication service providers in unlawfully disseminating the contents of electronic communications under ECPA. Freeman v. DirecTV, Inc., 457 F.3d 1001, 1004-09 (9th Cir. 2006).

Case3:08-cv-04373-JSW Document102 Filed09/12/12 Page25 of 62

makes clear that section 702 was "not intended to permit suit in circumstances where statutes
forbid or limit the relief sought. Clause (2) of section 702 contains a second proviso
concerned with situations in which Congress has consented to suit and the remedy provided is
intended to be the exclusive remedy. For example, in the Court of Claims Act, Congress created
a damage remedy for contract claims The measure is intended to foreclose specific
performance of government contracts. In terms of the proviso, a statute granting consent to suit,
i.e., the Tucker Act, 'impliedly forbids' relief other than the remedy provided by the Act." H.R.
Rep. No. 94-1656, p. 12-13 (1976), 1976 WL 14066, * 12-13. See also Block v. North Dakota ex
rel. Bd. of University and School Lands, 461 U.S. 273, 286 n. 22 (1983) ("§ 702 provides no
authority to grant relief 'when Congress has dealt in particularity with a claim and [has] intended
a specified remedy to be the exclusive remedy") (quoting H.R. Rep. No. 94-1656, p. 13).

Other statutes expressly or impliedly forbid the relief plaintiffs seek for the reasons discussed above. As noted above, other statutes expressly or impliedly forbid the relief plaintiffs seek. In 18 U.S.C. § 2712(a), Congress enacted a statutory scheme in which money damages would be available from the United States only for certain willful violations of FISA, the Wiretap Act, and the ECPA involving the use and disclosure of information, not collection, thereby "impliedly forbid[ding] relief other than the remedy provided." H.R. Rep. No. 94-1656, 1976 WL 14066, * 13. Plus, Congress added that this was to be the exclusive remedy against the United States. *See* § 2712(d). Equitable relief would be available from persons or entities other than the United States for Wiretap Act and ECPA violations. 18 U.S.C. §§ 2520 and 2707 expressly forbid equitable relief for Wiretap Act and ECPA violations from the United States.

The fact that plaintiffs have sued federal officials in their official capacity does not

⁸ 50 U.S.C. § 1810 creates a cause of action for certain FISA violations, but not against the United States, *see Al-Haramain*, and only for actual and punitive damages, attorney's fees and costs (not for equitable relief).

Case3:08-cv-04373-JSW Document102 Filed09/12/12 Page26 of 62

change the analysis. Plaintiffs cannot rely on Larson v. Domestic & Foreign Commerce Corp.,
337 U.S. 682 (1949), as a basis for their claims for equitable relief against the Government. See
Complaint at ¶¶ 155, 182, 219, and 242. In Larson, the Supreme Court held that a suit against a
federal official in his official capacity was a suit against the United States and was thus barred by
sovereign immunity. Id. at 703. The Court noted that "[t]here may be, of course, suits for
specific relief against officers of the sovereign which are not suits against the sovereign" and not
barred by sovereign immunity. <i>Id.</i> at 689. Included in the examples it provided was "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 his 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." <i>Id</i> .
In such cases, "the relief can be granted, without impleading the sovereign, only because of the
officer's lack of delegated power. A claim of error in the exercise of that power is therefore not
sufficient." Id. at 690. See also Dugan v. Rank, 372 U.S. 609 (1963).
Congress specifically addressed the Larson doctrine, however, when it amended section

Congress specifically addressed the *Larson* doctrine, however, when it amended section 702 of the APA in 1976 by adding the waiver of sovereign immunity it now contains. Congress recognized that actions for declaratory or injunctive relief against a named federal official had been allowed to proceed "on the theory he is exceeding his legal authority. In theory such actions are against the officer and not against the Government for whom he is acting and is a legal fiction developed by the courts to mitigate the injustice caused by strict application of the sovereign immunity doctrine." H.R. Rep. No. 94-1656, 1976 WL14066 * 5. Courts had applied this complicated legal fiction inconsistently and haphazardly, and Congress amended section 702 specifically to address this situation, effectively repealing the *Larson* exception. *Id.* at * 5-10. *See Schnapper v. Foley*, 667 F.2d 102, 108 (D.C. Cir. 1981) ("The clarity and force of the

Case3:08-cv-04373-JSW Document102 Filed09/12/12 Page27 of 62

legislative history leaves this court with no alternative but to conclude that all questions of the amenability of a federal officer to a suit for injunctive relief must be decided with reference to section 702, not *Larson*.").

The Ninth Circuit has explained that while it followed the legal fiction of *Larson* in cases prior to 1976, after 1976 it looks instead to section 702 of the APA, including the exceptions therein, for a waiver of sovereign immunity for equitable relief claims. *E.E.O.C. v. Peabody*Western Coal Co., 610 F.3d 1070, 1085 (9th Cir. 2010); *Presbyterian Church (U.S.A.) v. United*States, 870 F.2d 518, 524-26 (9th Cir. 1989). See also Geyen v. Marsh, 775 F.2d 1303, 1307 (5th Cir. 1985) ("The principal purpose of [the 1976 enactment of § 702's waiver] was to do away with the . . . [Larson] fiction[] surrounding sovereign immunity."); Sea-Land Serv., Inc. v. Brown, 600 F.2d 429, 432 (3d Cir. 1979) (observing the 1976 APA amendment "in effect repealed" the Larson exception); but see, e.g., Chamber of Commerce v. Reich, 74 F.3d 1322, 1328-29 (D.C Cir. 1996) (applying the Larson analysis after the 1976 amendments).

Even if *Larson* retained any vitality in the Ninth Circuit, which it does not, it would be inapplicable here. The named federal officials clearly have statutory authority to conduct electronic surveillance; plaintiffs' claim is that they violated that authority. *Larson*, 337 U.S. at 690. In addition, the effect of the equitable relief plaintiffs seek would run against the United States, preventing *Larson*'s application. *See Pennhurst State School & Hosp. v. Halderman*, 465 U.S. 89, 107 (1984). Plaintiffs seek to halt alleged widespread intelligence-gathering activity of the United States, and thus there is no question that plaintiffs seek relief that "would . . . restrain the Government from acting, or . . . compel it to act," or "interfere with public administration." *Pennhurst*, 465 U.S. at 102 n. 11 (quoting *Dugan*, 372 U.S. at 620); *see also Hawaii v. Gordon*, 373 U.S. 57, 58 (1963). The Ninth Circuit has repeatedly dismissed such *ultra vires* theories. *See Cent. Res. Life of North America Ins. Co. v. Struve*, 852 F.2d 1158, 1159-60, 1161 (9th Cir.

Case3:08-cv-04373-JSW Document102 Filed09/12/12 Page28 of 62

1988) (holding that "it cannot be seriously maintained" that a suit seeking an injunction ordering a state official to approve the marketing of insurance within the state was not against the sovereign); *Aminoil U.S.A., Inc. v. Cal. State Water Ctrl. Bd.*, 674 F.2d 1227, 1234 (9th Cir. 1982) (holding that a suit nominally against a federal official, which sought a determination that the official acted beyond the scope of his statutory authority was, in reality, a suit against the United States that would "preclude the [official] in his official capacity from enforcing the [law]."); *see also Palomar Pomerado Health Sys. v. Belshe*, 180 F.3d 1104, 1108 (9th Cir. 1999) (holding that where plaintiff sought an injunction that would restrain a state from reducing medical payment rates charged by plaintiff, relief would interfere with public administration and was thus barred absent waiver of sovereign immunity).

For the foregoing reasons, plaintiffs' statutory claims for declaratory and injunctive relief against the Government, presented in Counts V, VII, X, XIII and XVI, should be dismissed.

III. THE STATE SECRETS PRIVILEGE BARS THIS CASE FROM PROCEEDING.

Aside from the jurisdictional defects of plaintiffs' statutory claims against the Government, litigation of any of plaintiffs' claims in this case would require or risk the disclosure of information properly protected by the Government's assertion of the state secrets privilege and related statutory privileges. Plaintiffs' complaint quite clearly seeks disclosure of whether or to what extent the Government may have utilized certain intelligence sources and methods after the 9/11 attacks with the alleged assistance of particular telecommunications providers. It also seeks disclosure of whether any of the alleged activities (if they exist) are ongoing. As set forth below, the DNI, supported by the NSA, has properly asserted the state secrets privilege to protect such information from disclosure in order to prevent exceptionally grave damage to national security. Because the privileged information is central to plaintiffs' claims, all claims against all defendants (including the individual capacity defendants) must be

Case3:08-cv-04373-JSW Document102 Filed09/12/12 Page29 of 62

dismissed to protect the nation's security.

A. The State Secrets Privilege.

"The Supreme Court has long recognized that in exceptional circumstances courts must act in the interest of the country's national security to prevent disclosure of state secrets, even to the point of dismissing a case entirely." *Mohamed v. Jeppesen Dataplan, Inc.*, 614 F.3d 1070, 1077 (9th Cir. 2010) (en banc). The state secrets privilege has two overarching applications—both of which apply here. First, the privilege completely bars litigation of claims premised on state secrets where the very subject matter of the action would require the disclosure of state secrets. *See Tenet v. Doe*, 544 U.S. 1, 8-10 (2005) (barring suit against the Government to enforce covert espionage agreements); *Weinberger v. Catholic Action of Hawaii/Peace Education Project*, 454 U.S. 139, 146-47 (1981) (barring suit to compel the Navy to prepare environmental impact statement for facility where Navy allegedly proposed to store nuclear weapons, where, due to national security reasons, the Navy could neither admit nor deny the allegation); *Totten v. United States*, 92 U.S. 105, 107 (1875) (barring suit against the Government for breach of secret agreement to compensate spy).

Second, the state secrets privilege excludes evidence protected by the privilege. *See United States v. Reynolds*, 345 U.S. 1 (1953). When the case cannot proceed without the privileged evidence, or when litigating the case to judgment on the merits would present an unacceptable risk of disclosing state secrets, it must be dismissed. *Jeppesen*, 614 F.3d at 1079, 1083, 1087-90 (dismissing claims against company that allegedly provided flight planning and other services in support of government's alleged extraordinary rendition program, because litigating case would present unacceptable risk of disclosing state secrets). *See also General Dynamics Corp. v. United States*, 131 S. Ct. 1900, 1907 (2011) ("Where liability depends upon the validity of a plausible . . . defense, and when full litigation of that defense would inevitably

Case3:08-cv-04373-JSW Document102 Filed09/12/12 Page30 of 62

lead to the disclosure of state secrets, neither party can obtain judicial relief.") (internal quotation and citation omitted).

There is no rigid dichotomy between a *Totten* and *Reynolds* dismissal. The Ninth Circuit has observed that "a bright line does not always separate the subject matter of the lawsuit from the information necessary to establish a prima facie case." *Al-Haramain Islamic Foundation, Inc. v. Bush*, 507 F.3d 1190, 1205 (9th Cir. 2007). In some cases, "there may be no dividing line" while, in other cases, "the suit itself may not be barred because of its subject matter and yet ultimately, the state secrets privilege may nonetheless preclude the case from proceeding to the merits." *Id.* (describing "continuum of analysis"). Dismissal is required where "the claims and possible defenses are so infused with state secrets that the risk of disclosing them is both apparent and inevitable." *Jeppesen*, 614 F.3d at 1089. "Dismissal under these circumstances, like dismissal under the *Totten* bar, reflects the general principle" that public policy forbids the maintenance of any suit that would inevitably lead to the disclosure of national security information. *See id.*9

18

19

20

21

22

23

24

25

26

1

2

3

4

5

6

7

9

10

11

12

13

14

15

16

¹⁷

⁹ Plaintiffs suggest that the Supreme Court, in *General Dynamics*, "effectively overruled" the Ninth Circuit's holding in Jeppesen that the state secrets privilege requires dismissal when there is an unacceptable risk that state secrets will be disclosed, or when the very subject matter of the action would require the disclosure of state secrets. See Pls. Mem. at 11. Plaintiffs misread General Dynamics, which is a narrow decision that involved consideration of the use of the privilege "only where it precludes a valid defense in Government-contracting disputes." See 131 S.Ct. at 1910; see also id. at 1909 (the rule announced applies only to the superior knowledge defense" in government contracting disputes). Because a classified contractor relationship was at issue, the court looked principally to the Totten doctrine to decide the case and ultimately decided to "leave the parties where it found them." See id. at 1906-09. Also, the fact that General Dynamics was resolved with reference to "commonlaw authority to fashion contractual remedies in Government-contracting disputes," id. at 1906, does not mean it restricted application of the state secrets privilege to that type of case, and it certainly did not "overrule" Jeppesen. Plaintiffs' argument is merely another attempt to limit the reach of the state secrets privilege to the causes of action in which it has been litigated, but courts have repeatedly rejected this cramped reading of the privilege. Tenet, 544 U.S. at 8 (rejecting argument that *Totten* applies only to breach-of-contract claims); id. ("'[P]ublic policy forbids the maintenance of any suit in a court of justice, the trial of which would inevitably lead to the disclosure of matters which the law itself regards as confidential.") (quoting Totten, 92 U.S. at 107 (emphasis added by Tenet court); Al-Haramain, 507 F.3d at 1205 (holding that constitutional and statutory claims against government for alleged warrantless electronic surveillance program must be dismissed because plaintiffs could not establish standing without evidence precluded by the state secrets privilege, unless FISA preempts the privilege).

Case3:08-cv-04373-JSW Document102 Filed09/12/12 Page31 of 62

The Government may assert a *Reynolds* privilege claim "at any time, even at the pleading stage," and need not wait for an evidentiary dispute to arise. *Jeppesen*, 614 F.3d at 1080-81. In analyzing such an assertion, the Court must ensure that the Government has satisfied the procedural requirements for invoking the state secrets privilege, make an independent determination that the information is privileged, and resolve how the matter should proceed in light of the successful privilege claim. *Id.* at 1080.

1. Procedural Requirements

The state secrets privilege is "not to be lightly invoked." *Jeppesen*, 614 F.3d at 1080 (quoting *Reynolds*, 345 U.S. at 7). To make sure that the privilege is invoked only when necessary, the Government "there must be a formal claim of privilege, lodged by the head of the department which has control over the matter, after actual personal consideration by that officer." *Id.* (quoting *Reynolds*, 345 U.S. at 7-8).

2. The Court's Independent Evaluation of the Privilege Claim

The privilege claim must be sufficiently detailed to permit the Court's independent determination of it. *Jeppesen*, 614 F.3d at 1080. The privilege must be sustained when the court is satisfied, "from all the circumstances of the case, that there is a reasonable danger that compulsion of the evidence will expose . . . matters which, in the interest of national security, should not be divulged." *Reynolds*, 345 U.S. at 10. "If this standard is met, the evidence is absolutely privileged, irrespective of the plaintiffs' countervailing need for it." *Jeppesen*, 614 F.3d at 1081 (citing *Reynolds*, 345 U.S. at 11 ("[E]ven the most compelling necessity cannot overcome the claim of privilege if the court is ultimately satisfied that [state] secrets are at stake.")). In evaluating the need for secrecy, courts must "acknowledge the need to defer to the Executive on matters of foreign policy and national security and surely cannot legitimately find ourselves second guessing the Executive in this arena." *Al-Haramain*, 507 F.3d at 1203. At the

Case3:08-cv-04373-JSW Document102 Filed09/12/12 Page32 of 62

same time, "the state secrets doctrine does not represent a surrender of judicial control over access to the courts," *Jeppesen*, 614 F.3d at 1082, and "to ensure that the state secrets privilege is asserted no more frequently and sweepingly than necessary, it is essential that the courts continue critically to examine instances of its invocation." *Id.* (internal quotations and citation omitted).

3. Impact of Privilege Assertion on the Case

When a court sustains a claim of privilege, it must then resolve how the matter should proceed in light of the successful privilege claim. When successfully invoked, the evidence subject to the privilege is "completely removed from the case." *Kasza v. Browner*, 133 F.3d 1159, 1166 (9th Cir. 1998). In the normal course, after the privileged evidence is excluded, "the case will proceed accordingly, with no consequences save those resulting from the loss of evidence." *Al-Haramain*, 507 F.3d at 1204 (quoting *Ellsberg v. Mitchell*, 709 F.2d 51, 64 (D.C. Cir. 1983)). In some cases, however, "application of the privilege may require dismissal of the action." *Jeppesen*, 614 F.3d at 1083. "When this point is reached, the *Reynolds* privilege converges with the *Totten* bar, because both require dismissal." *Id*.

First, "if '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." *Jeppesen*, 614 F.3d at 1083 (quoting *Kasza*, 133 F.3d at 1166).

Similarly, if the plaintiff cannot establish her standing without the excluded state secrets, then the privilege assertion requires dismissal. *Al-Haramain*, 507 F.3d at 1204-05. Second, "if the privilege deprives the defendant of information that would otherwise give the defendant a valid defense to the claim, then the court may grant summary judgment to the defendant." *Jeppesen*, 614 F.3d at 1083 (quoting *Kasza*, 133 F.3d at 1166) (internal quotations omitted). And third, "even if the claims and defenses might theoretically be established without relying on privileged

Case3:08-cv-04373-JSW Document102 Filed09/12/12 Page33 of 62

evidence, it may be impossible to proceed with the litigation because—privileged evidence being inseparable from nonprivileged information that will be necessary to the claims or defenses—litigating the case to a judgment on the merits would present an unacceptable risk of disclosing state secrets." *Id.*; *see also El-Masri v. United States*, 479 F.3d 296, 308 (4th Cir. 2007) ("[A] proceeding in which the state secrets privilege is successfully interposed must be dismissed if the circumstances make clear that privileged information will be so central to the litigation that any attempt to proceed will threaten that information's disclosure."); *Fitzgerald v. Penthouse Int'l*, *Ltd.*, 776 F.2d 1236, 1241-42 (4th Cir. 1985) ("[I]n some circumstances sensitive military secrets will be so central to the subject matter of the litigation that any attempt to proceed will threaten disclosure of the privileged matters."); *accord Farnsworth Cannon, Inc. v. Grimes*, 635 F.2d 268, 279-81 (4th Cir. 1980) (*en banc*).

4. The Attorney General's Policy

In addition to these judicial standards, under 2009 policy issued by the Attorney General governing the assertion and defense of the state secrets privilege in litigation, the Department of Justice will defend an assertion of the state secrets privilege in litigation, and seek dismissal of a claim on that basis, only when "necessary to protect against the risk of significant harm to national security." Policies and Procedures Governing Invocation of the State Secrets Privilege at 1, available at http://www.justice.gov/opa/documents/state-secret-privileges.pdf. Moreover, "[t]he Department will not defend an invocation of the privilege in order to: (i) conceal violations of the law, inefficiency, or administrative error; (ii) prevent embarrassment to a person, organization, or agency of the United States government; (iii) restrain competition; or (iv) prevent or delay the release of information the release of which would not reasonably be expected to cause significant harm to national security." *Id.* at 2.

The Attorney General's policy also established detailed internal procedures for review of

Case3:08-cv-04373-JSW Document102 Filed09/12/12 Page34 of 62

a proposed assertion of the state secrets privileged in a particular case. Those procedures require submissions by the relevant government departments or agencies specifying "(i) the nature of the information that must be protected from unauthorized disclosure; (ii) the significant harm to national security that disclosure can reasonably be expected to cause; [and] (iii) the reason why unauthorized disclosure is reasonably likely to cause such harm." *Id.* The Department will defend an assertion of the privilege in court only with the personal approval of the Attorney General following review and recommendations from senior Department officials. *Id.* at 3.

B. Plaintiffs' Allegations of Dragnet Surveillance Program Cannot Be Litigated Without Information Over Which The United States Has Properly Asserted The State Secrets Privilege.

The United States has properly asserted and supported the state secrets privilege in this case. The DNI, who heads the United States Intelligence Community, *see* 50 U.S.C. § 403 (b)(1); *Al-Haramain*, 507 F.3d at 1202 & n. 6, has formally asserted the state secrets privilege after actual personal consideration of the matter. *See* Public and Classified *In Camera*, *Ex Parte* Declarations of James R. Clapper, Director of National Intelligence. The DNI's assertion of the privilege is further supported by a declaration from the NSA. *See* Public and Classified *In Camera*, *Ex Parte* Declarations of Frances Fleisch, National Security Agency.

Through these declarations, the Government has asserted the state secrets privilege (as well as other statutory privileges) over (1) information that may tend to confirm or deny whether plaintiffs have been subject to any alleged NSA intelligence activity that may be at issue in this case; (2) any information concerning NSA intelligence activities, sources, or methods that may relate to or be necessary to litigate plaintiffs' claims, including allegations that NSA, with the assistance of telecommunications carriers such as AT&T and Verizon, indiscriminately intercepts the content of communications and collects communication transactional records of millions of Americans as part of an alleged presidentially authorized program after 9/11. The DNI and NSA privilege assertions include information about the scope and operation of the

Case3:08-cv-04373-JSW Document102 Filed09/12/12 Page35 of 62

TSP,¹⁰ other information related to demonstrating that the NSA does not engage in the content surveillance dragnet alleged by plaintiffs, information about whether NSA obtained communication transactional records from telecommunications companies such as AT&T or Verizon, and information that may tend to confirm or deny whether any particular telecommunications company has provided assistance to the NSA in connection with any alleged activity.¹¹

The Government has amply demonstrated in the DNI and NSA public and classified declarations that disclosure of the privileged information reasonably could be expected to cause exceptionally grave damage to national security. The disclosure of information concerning whether plaintiffs have been subject to alleged NSA intelligence activity would necessarily reveal NSA intelligence sources and methods, including whether certain intelligence collection activities existed and the nature of any such activity. The disclosure of whether specific individuals were targets of alleged NSA activities would also reveal who is subject to investigative interest—helping that person to evade surveillance—or who is not—thereby revealing the scope of intelligence activities as well as the existence of secure channels for communication. *See* Public DNI Decl. ¶ 22; Public NSA Decl. ¶ 16-17. *See also Al-Haramain*, 507 F.3d at 1203.

Intelligence Surveillance Court had been issued and authorized the Government to target for collection certain international communications into or out of the United States where there is probable cause to believe that one of the communicants is a member or agency of al Qaeda or an affiliated terrorist organization; that, as a result of these orders, any electronic surveillance that had been occurring as part of the TSP was then being conducted subject to the approval of the FISA court; and that, under these circumstances, the TSP was not reauthorized. *See* NSA Decl. ¶ 15, n.5. While plaintiffs do not allege they were subject to TSP surveillance, the operational details of that program remain classified and subject to the DNI's privilege assertion. *See* Public DNI ¶ 23. In addition, as noted above, in July 2008 Congress enacted the FISA Amendments Act of 2008, which established new FISA authority to undertake electronic surveillance directed at non-U.S. persons located outside the United States. *See* 50 U.S.C. § 1881a, *et seq.* Again, plaintiffs do not challenge any surveillance under this authority, and the particular sources and methods by which it is conducted likewise are classified and privileged.

¹¹ In addition, the DNI has asserted privilege over classified information concerning the specific nature of the terrorist threat posed by al Qaeda and its affiliates and other threats to the United States. See Public DNI Decl. ¶ 11(A); 21. Such information is crucial to understanding the important to our national security of the NSA intelligence activities, sources, and methods implicated by plaintiffs' allegations but cannot be disclosed without causing exceptionally grave danger to national security. *Id*.

Case3:08-cv-04373-JSW Document102 Filed09/12/12 Page36 of 62

In addition, the disclosure of other privileged information in litigating plaintiffs' allegation that the NSA has intercepted the communications content and obtained the communications transactional records of millions of Americans, as part of an alleged presidentially-authorized program after 9/11, reasonably could be expected to cause exceptionally grave damage to national security. The DNI explains that, as the Government has previously indicated, the NSA's collection of the content¹² of communications under the now inoperative TSP was directed at international communications in which a participant was reasonably believed to be associated with al Qaeda or an affiliated terrorist organization, and thus plaintiffs' allegation that the NSA has indiscriminately collected the content of millions of communications sent or received by people inside the United States after 9/11 under the TSP is false. See Public DNI ¶ 24; Public NSA Decl. ¶ 18. But attempting to demonstrate that the TSP was not the content dragnet plaintiffs allege, or that the NSA has not otherwise engaged in a content dragnet, would risk or require the disclosure of highly classified NSA intelligence sources and methods about the TSP and other NSA activities, causing exceptionally grave damage to national security. See Public DNI Decl. ¶ 24; Public NSA Decl. ¶ 18.

The DNI has also explained that confirmation or denial of whether the NSA has collected communication records would cause exceptional harm to national security by disclosing whether or not NSA utilizes certain intelligence sources and methods, thereby revealing NSA's capabilities and operations, or the lack thereof, information that foreign adversaries could exploit. See Public DNI Decl. ¶ 25; Public NSA Decl. ¶ 20. See Terkel v. AT&T Corp., 441 F. Supp. 2d 899, 917 (N.D. Ill. 2006) (addressing an identical allegation, upholding the Government's state secrets privilege assertion to preclude disclosure of whether the Government was obtaining large quantities of communications records, information that would have allowed adversaries to gain valuable insight into the Government's intelligence activities); *Hepting*, 439

26

27

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

The term "content" is used herein to refer to the substance, meaning or purport of a communication, as defined in 18 U.S.C. § 2510(8). See Public DNI Decl. ¶ 23, n.1.

Case3:08-cv-04373-JSW Document102 Filed09/12/12 Page37 of 62

F. Supp. 2d at 997 (preventing discovery into allegations concerning communications records, noting that the Government has neither confirmed nor denied whether it monitors communications records).

Litigation of the plaintiffs' claims would also plainly risk or require the disclosure of whether particular telecommunications carriers, including AT&T or Verizon, assisted the Government in alleged intelligence activities. Plaintiffs clearly allege such assistance, and any attempt to address their claims would encounter privileged information concerning the role, if any, of particular telecommunications providers. The DNI again has demonstrated that disclosure of whether the NSA has an intelligence relationship with a particular telecommunications company reasonably could be expected to cause exceptionally grave damage to national security—among other reasons, by revealing to foreign adversaries which channels of communication may or may not be secure. *See* Public DNI Decl. ¶ 26; Public NSA Decl. ¶¶ 21-22.

Notably, in enacting the FISA Act Amendments Act of 2008, the Senate Select Committee on Intelligence ("SSCI") found that "[t]he details of the President's program are highly classified. As with other intelligence matters, the identities of persons or entities who provide assistance to the U.S. Government are protected as vital sources and methods of intelligence....It would be inappropriate to disclose the names of the electronic communication service providers from which assistance was sought, the activities in which the Government was engaged or in which providers assisted, or the details regarding any such assistance." S. Rep. 110-209, 2007 WL 5334390, at 7 (110th Cong., 1st Sess. 2007). See also Terkel, 441 F. Supp. 2d at 917 (upholding the Government's privilege assertion over whether AT&T had disclosed

The Government does not contend that the plaintiffs' claims against the Government are foreclosed by the FAA. We simply observe that this litigation puts squarely at issue the information Congress sought to protect through the FAA—"the names of the electronic communication service providers from which assistance was sought, the activities in which the Government was engaged or in which providers assisted, or the details regarding any such assistance." *See* S. Rep. 110-209 at 9.

Case3:08-cv-04373-JSW Document102 Filed09/12/12 Page38 of 62

communications records to the Government).¹⁴

Accordingly, attempting to litigate this matter to a judgment on the merits would present an unacceptable risk of disclosing state secrets. *Jeppesen*, 614 F.3d at 1083. On the face of the complaint, it is apparent that plaintiffs seek to put at issue NSA intelligence sources and methods allegedly used after the 9/11 attacks and the identities of any telecommunication carriers that may have assisted the Government. Properly privileged information is not at the periphery of the case: the very purpose of the litigation is to obtain the disclosure of NSA sources and methods in order to probe into their lawfulness. The DNI and NSA privilege assertions, including their classified submissions, set forth in detail the information plainly at risk of disclosure and the exceptional damage to national security that would result from disclosure.

Moreover, the existence of public speculation about alleged NSA activities in media reports, or by plaintiffs' own declarants, does not diminish the need to protect the intelligence sources and methods at issue. As the NSA explains, the "process of sorting out whether any allegation is true, partly true, or wholly false, would necessarily risk or require disclosure of the intelligence sources and methods and confirm to our adversaries whether or not, or to what extent, the NSA utilizes certain sources and methods, and thereby reasonably could be expected to cause exceptionally grave damage to national security." *See* Public NSA Decl. ¶ 4; Public DNI

Litigation of plaintiffs' allegations concerning telecommunications carriers is foreclosed not only by operation of the state secrets privilege, but also directly by the *Totten/Tenet* doctrine as well. *Tenet*, 544 U.S. at 11 ("The possibility that a suit may proceed and an espionage relationship may be revealed, if the state secrets privilege is not found to apply, is unacceptable: Even a small chance that some court will order disclosure of a source's identity could well impair intelligence gathering and cause sources to 'close up like a clam.'") (internal quotations and citation omitted).

¹⁵ Aside from being wholly speculative, plaintiffs' declarations all rely on inadmissible hearsay as to what the declarants have allegedly been told. For example, Mr. Drake admits that he was not read into the alleged President's Surveillance Program, but nonetheless states that "various NSA employees who were implementing various aspects of the PSP confided in me and told me that the PSP involved the collection of domestic electronic communications traffic without any privacy protections or judicial oversight." Drake Declaration at ¶ 7. See also Binney Declaration at ¶ 5. The statements are offered for the truth of the matters asserted therein, and are thus inadmissible hearsay. See Fed. R. Evid. 801, 802. In addition, plaintiffs' declarations rely on media reports and publications for the truth of the matters asserted therein, which also constitute inadmissible hearsay.

Case3:08-cv-04373-JSW Document102 Filed09/12/12 Page39 of 62

Decl. ¶ 3. In this case, "the claims and possible defenses are so infused with state secrets that the risk of disclosing them is both apparent and inevitable." *Jeppesen*, 614 F.3d at 1089. Adversarial litigation is "inherently complex and unpredictable," and "where the relevant secrets are difficult or impossible to isolate . . . even efforts to define a boundary between privileged and unprivileged evidence would risk disclosure by implication." *Id*.

Beyond the unacceptable risk of disclosing sensitive sources and methods of intelligence collection, it should also be apparent that plaintiffs could not establish their own individual standing to sue without information about whether they were in fact subject to surveillance. Plaintiffs, of course, bear the burden of establishing standing and must demonstrate (1) an injury-in-fact, (2) a causal connection between the injury and the conduct complained of, and (3) a likelihood that the injury will be redressed by a favorable decision. *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 559-60 (1992). In meeting this burden, plaintiffs must demonstrate an actual or imminent—not speculative or hypothetical—injury that is particularized as to them; they cannot rely on alleged injuries to unnamed members of a purported class. *See, e.g., Warth v. Selden*, 422 U.S. 490, 502 (1975); *see also Ellsberg*, 709 F.2d at 65. Plaintiffs cannot rest on general allegations in their complaint, but must be able to set forth specific facts that establish their standing to obtain the relief sought. *See Lewis v. Casey*, 518 U.S. 343, 358 (1996) (quoting *Lujan*, 504 U.S. at 561).

For each cause of action, plaintiffs must establish that they have been "aggrieved"—that is, subject to the alleged action being challenged. But information concerning whether

With respect to plaintiffs' claim for damages under FISA Section 1810, the term "aggrieved person" is "coextensive [with], 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); see also Rakus v. Illinois, 439 U.S. 128, 132, n. 2 (1978) (a party raising a Fourth Amendment claim "must allege such a personal stake or interest in the outcome of the controversy as to assure the concrete adverseness which Art. III requires."). Similarly, under the Wiretap Act, 18 U.S. C. § 2510, civil actions may be brought only by a "person whose . . . communication is intercepted, disclosed, or intentionally used." 18 U.S.C. § 2520(a). The Stored Communication Act likewise (cont'd)

Case3:08-cv-04373-JSW Document102 Filed09/12/12 Page40 of 62

plaintiffs have been surveilled by the NSA is specifically protected by the Government's state				
secrets assertion. Because plaintiffs cannot adduce proof that the content of their				
communications or their communications records have been collected by the Government, the				
most basic element of every claim—their standing as "aggrieved persons"—cannot be				
established, and even if plaintiffs attempted to do this by public information, the Government				
could not address or refute their evidence without information subject to the privilege. See				
ACLU v. NSA, 493 F.3d at 656 (Batchelder, J.) (where state secrets privilege prevents discovery				
of evidence of standing, allegations of harm held to be speculative and insufficient to support				
standing); id. at 692 (Gibbons, J. concurring) (dismissal required where state secrets privilege				
prevents plaintiffs from establishing whether they were subject to TSP or government from				
presenting evidence to refute that allegation); <i>Terkel</i> , 441 F. Supp. 2d at 919-20 (dismissing				
claim alleging that AT&T had disclosed communication records to the Government because state				
secrets privilege foreclosed plaintiffs from establishing their standing). Nor can plaintiffs avoid				
this obstacle by claiming that NSA unlawfully intercepted the communications of millions of				
Americans with the assistance of AT&T or Verizon, and plaintiffs are AT&T or Verizon				
customers. Plaintiffs must establish their own personal injury and cannot do so without properly				
privileged information.				

In addition, beyond questions of standing, the merits of plaintiffs' claims cannot be litigated without the privileged information. The Government has asserted the state secrets privilege over the information necessary to prove or disprove plaintiffs' claims that the NSA, with assistance from particular telecommunications providers, conducted a dragnet collection of the content of communications and of communications records. For example, plaintiffs' Wiretap Act claim would require proof that one of plaintiffs' wire or electronic communications, as defined in the Act (*see* 18 U.S.C. § 2510 (1), (12)), had been intercepted—information that

limits civil remedies to "person[s] aggrieved" under the statute, id. § 2707(a); *see id.* 2711(1) (adopting § 2510(11) definition of "aggrieved person" as one "who was a party to any intercepted . . . communication" or "a person against whom the interception was directed"). Each of these provisions reflects the fundamental point that only persons who can establish factually that their own rights were injured by the actual interception or disclosure of their own communications (or records) have Article III standing to proceed.

Case3:08-cv-04373-JSW Document102 Filed09/12/12 Page41 of 62

would reveal whether or not particular intelligence methods were utilized and conducted through a particular carrier.

Similarly, for their ECPA claims, plaintiffs would have to show that the Government required an electronic communication service provider to disclose the content of plaintiffs' communications in electronic storage, and whether or not such a disclosure occurred pursuant to a court order or statutory authority. *See* 18 U.S.C. § 2703(a), (b). With respect to plaintiffs' ECPA claim concerning the alleged collection of communication records, *see* 18 U.S.C. § 2703(c), not only must there be official confirmation or denial of the existence of the alleged activity but, if that activity were confirmed, plaintiffs would have to adduce proof concerning the scope and operation of any such program, including, for example, whether it actually encompassed plaintiffs' records, when and how it may have done so, and again whether any such action was authorized by court order or statute.

Plaintiffs' related Fourth and First Amendment claims both put at issue not only whether plaintiffs' individual communications (content or records) were collected, but whether there existed a reasonable basis for the particular search or seizure, whether exigent circumstances warranted any action at issue, and what specific information was obtained by the Government. Fourth Amendment claims require fact-specific determinations, including whether a search was undertaken, under what authority, whether it violated an expectation of privacy, and why the Government may have acted. *See, e.g., O'Connor v. Ortega*, 480 U.S. 709, 719 (1987) ("what is reasonable depends on the context within which a search takes place") (quoting *New Jersey v. T.L.O.*, 469 U.S. 325, 337 (1985)). And if the Government obtained only non-content informational records, there may be no Fourth Amendment issue at all, ¹⁷ but even that proposition could not be addressed without the disclosure of properly privileged information.

¹⁷ See Smith v. Maryland, 442 U.S. 735, 742-46 (1979) (holding that individuals have no legitimate expectation of privacy in the numbers they dial on the telephone, and a pen register search of such information does not constitute a search for Fourth Amendment purposes); *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008) ("[E]-mail and Internet users have no expectation of privacy in the to/from addresses of their messages or the IP addresses of the websites they visit because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information.").

Case3:08-cv-04373-JSW Document102 Filed09/12/12 Page42 of 62

Finally, adjudication of the merits as well as plaintiffs' standing to obtain prospective relief in particular would require disclosure of whether any of the alleged activities (if they exist) are ongoing, occurred only during certain periods, or were authorized at some point by statute, court order, or other authority. Such disclosures again would reveal a range of facts concerning whether, when, how, why, and under what authority the NSA may have utilized certain intelligence sources and methods—information that is subject to the Government's privilege assertion and cannot be disclosed without risking exceptionally grave damage to national security. The exclusion of this information from the case pursuant to the state secrets privilege precludes the litigation of plaintiffs' claims, including their claims for prospective relief for which they must show that they are currently subject to an alleged activity or otherwise "immediately in danger of sustaining some direct injury" as the result of the challenged conduct. City of Los Angeles v. Lyons, 461 U.S. 95, 102 (1983).

In sum, the Government has demonstrated that the privileged information identified by the DNI and NSA is properly excluded from this case, and that the risk of its disclosure exists at all stages as to all claims, and, accordingly that dismissal of this litigation is required.

IV. PLAINTIFFS' MOTION FOR PARTIAL SUMMARY JUDGMENT SHOULD BE DENIED BECAUSE LITIGATION OF PLAINTIFFS' CLAIMS MAY NOT PROCEED UNDER FISA.

To counter the Government's reassertion of the state secrets privilege, plaintiffs contend that the Foreign Intelligence Surveillance Act, 50 U.S.C.§ 1801, et seq., "displaces" the state secrets privilege as to all of their claims and, in its place, establishes procedures to be followed "in cases involving electronic surveillance." See Pls. Mem. at 12-22. Plaintiffs' FISA displacement theory is without merit.

In sum, plaintiffs first disregard the governing standard—namely, that displacement may be found only when a statutory provision speaks clearly and directly to the particular application of the common law at issue. Far from clearly addressing the issue, *nothing* in the FISA's text or legislative history provides any indication that Congress intended to override the Executive's

Case3:08-cv-04373-JSW Document102 Filed09/12/12 Page43 of 62

long-recognized ability to assert the state secrets privilege or to override the process established by the Supreme Court for invoking the privilege. In particular, nothing in subsection 106(f) of the FISA, 50 U.S.C. § 1806(f)—the provision plaintiffs rely on—speaks clearly or directly to the question. Rather, the procedures for *in camera, ex parte* judicial review in that provision apply to an entirely different scenario: when the use of evidence derived from electronic surveillance against an "aggrieved" person is at issue—*i.e.*, a person who is the "target of an electronic surveillance" or a "person whose communications or activities were subject to electronic surveillance." *See* 50 U.S.C. § 1801(k). Subsection 1806(f) does not permit a person who merely alleges he or she has been subject to electronic surveillance to discover whether that is so and then litigate the merits. Notably, legislative history for subsection 1806(f) makes clear that the Government may choose to protect intelligence sources and methods, and forego judicial review under that provision, by not using surveillance evidence against an aggrieved person in a particular proceeding. As set forth further below, the Court should reject plaintiffs' FISA displacement theory.¹⁸

A. Congress May Not Displace the Common Law Without a Clear Statement Addressing the Particular Question.

Whether the FISA displaces the state secrets privilege in the circumstances of this case turns on whether Congress has spoken to the matter clearly and directly. Nothing in the FISA indicates any intention by Congress—let alone a clear directive—to abrogate the state secrets privilege. Two related doctrines govern this issue.

First, in order to abrogate such a well-established common law principle as the state

Plaintiffs cite former Chief Judge Walker's decision *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 subsection 1806(f) displaces the state secrets privilege). *See* Pls. Mem. at 12 n.7. Judgment in *Al-Haramain* has now been vacated on other grounds. *See Al-Haramain Islamic Foundation, Inc. v. Bush*, 2012 WL 3186088. The Government continues to disagree with Judge Walker's analysis, as noted throughout below.

Case3:08-cv-04373-JSW Document102 Filed09/12/12 Page44 of 62

1

2

3

4

5

6

7

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

secrets privilege, a statute must "speak directly" to the question addressed by the common law. City of Milwaukee v. Illinois, 451 U.S. 304, 315 (1981); County of Oneida v. Oneida Indian Nation, 470 U.S. 226, 236-37 (1985); In re Hanford Nuclear Reservation Litigation, 497 F.3d 1005, 1018-19 (9th Cir. 2007). The state secrets privilege is deeply rooted in common law, Kasza, 133 F.3d at 1167-68, and "the common law . . . ought not to be deemed repealed, unless the language of a statute be clear and explicit for this purpose." Norfolk Redevelopment & Housing Auth. v. Chesapeake & Potomac Tel. Co., 464 U.S. 30, 35 (1983); see also United States v. Texas, 507 U.S. 529, 534 (1993); In re Niles, 106 F.3d 1456, 1461 (9th Cir. 1997). "Where a common-law principle is well established . . . the courts may take it as given that Congress has legislated with an expectation that the principle will apply except "when a statutory purpose to the contrary is evident." Astoria Fed. Sav. & Loan Ass'n v. Solimino, 501 U.S. 104, 108 (1991) (citation omitted). The Ninth Circuit has applied the "direct statement" standard in assessing whether statutory law displaces the state secrets privilege, Kasza, 133 F.3d at 1167. Accordingly, there can be no basis to conclude that Congress set aside the privilege through the FISA unless it did so in clear and explicit terms.

In addition, because the state secrets privilege has "a firm foundation in the Constitution, in addition to its basis in the common law of evidence," *El-Masri*, 479 F.3d at 303-04, a separate doctrine requires that statutes not be read to interfere with the President's powers unless Congress has made clear an intent to confront the ensuing constitutional questions. *See Franklin v. Massachusetts*, 505 U.S. 788, 800-01 (1992) (an express statement is required before concluding that Congress meant to regulate the President's exercise of his executive functions). ¹⁹

¹⁹ In *Franklin*, the Supreme Court held that the Administrative Procedure Act does not apply to the President, finding that "[o]ut of respect for the separation of powers and the unique constitutional position of the President, . . . textual silence is not enough to subject the President to the provisions of the APA. *Franklin*, 505 U.S. at 800. Likewise, in *Armstrong v. Bush*, 924 F.2d 282 (D.C. Cir. 1991), the D.C. Circuit rejected application of the (cont'd)

Case3:08-cv-04373-JSW Document102 Filed09/12/12 Page45 of 62

The state secrets privilege derives from the President's Article II powers, including his powers as Commander in Chief. *See United States v. Nixon*, 418 U.S. 683, 710 (1974); *cf. Department of the Navy v. Egan*, 484 U.S. 518, 527 (1988) (the Executive's authority to control access to information bearing on national security "exists quite apart from any explicit congressional grant" of power because it flows primarily from the "constitutional investment of power in the President" found in Article II of the Constitution).

Accordingly, displacement of the state secrets privilege cannot be found unless Congress made clear its intent to do so. As detailed below, neither the terms of FISA nor its legislative history references the state secrets privilege, and the terms of subsection 1806(f) cannot reasonably be construed to displace the privilege or permit discovery into whether someone has been subject to alleged surveillance.

Plaintiffs do not acknowledge the standard governing displacement of the common law, but instead assert that Rule 501 of the Federal Rules of Evidence applies. *See* Pls. Mem. at 13-14 &n.9. This contention is meritless. Rule 501 provides that "[t]he common law—as interpreted by United States courts in the light of reason and experience—governs a claim of privilege unless any of the following provides otherwise: [1] the United States Constitution; [2] a federal statute; or [3] rules prescribed by the Supreme Court." As a general matter, the language of FRE 501 provides that the common law governs unless it is otherwise displaced. The rule does not purport to address the standard of review governing whether a federal statute displaces a common law privilege or rule prescribed by the Supreme Court. Indeed, as the authority cited above indicates, the Supreme Court has repeatedly set forth the "clear statement" rule for

APA to Presidential action "[i]n the absence of any affirmative evidence that these issues were considered in the legislative process and that Congress passed the APA with the understanding that it would regulate presidential as well as other executive branch action. *Armstrong*, 924 F.2d at 288-90.

Case3:08-cv-04373-JSW Document102 Filed09/12/12 Page46 of 62

deciding displacement issues even after FRE 501 was adopted.²⁰

B. Congress' "Comprehensive" Regulation Of Foreign Intelligence Surveillance Does Not Displace The State Secrets Privilege.

Before addressing the particular terms of FISA subsection 1806(f), one aspect of plaintiffs' displacement theory may be dispensed with in short order. The fact that the FISA comprehensively regulates the Government's use of foreign intelligence electronic surveillance says nothing about whether the statute clearly and directly displaces the state secrets privilege in the particular circumstances of this litigation. *See* Pls. Mem. at 14-17.²¹

There is no question that Congress, through the FISA, established a detailed regime addressing foreign intelligence surveillance.²² But even in contexts where a "comprehensive" scheme of regulation is at issue, "[t]he test for whether congressional legislation excludes the declaration of federal common law is simply whether the statute 'speak[s] directly to [the] question' at issue." *American Elec. Power Co. v. Connecticut*, ---U.S.---, 2011 WL 2437011 *9 (U.S. June 20, 2011) (quoting *Mobil Oil Corp. v. Higginbotham*, 436 U.S. 618, 625 (1978)); *see also City of Milwaukee v. Illinois*, 451 U.S. at 313-14 (federal statute must "speak directly" to the "particular issue" to supplant common law).²³ Thus, the inquiry here is not whether the FISA

²⁰ Plaintiffs' citation to the legislative history of Rule 501 is equally unavailing. Reference to a privilege for "secrets of state" in the history of Rule 501 concerned the rejection of proposed statutory rules of evidence governing numerous privileges, including for state secrets, in favor of the more general rule adopted. *See* H.R. Rep. No. 93-650 (1973), reprinted in 1974 U.S.C.C.A.N. 7075, 7082; S. Rep. No. 93-1277 (1974); 1974 U.S.C.C.A.N. 7051, 7058 (same).

²¹ Judge Walker adopted a similar theory in reaching his now-vacated judgment in *Al-Haramain. See* 564 F. Supp. 2d at 1115-20. As set forth herein, that analysis was incorrect.

Among other things, FISA strictly defines "electronic surveillance" for foreign intelligence surveillance purposes, 50 U.S.C. § 1801(f); establishes a procedure for the Government, with the approval of the Attorney General, to apply for judicial orders authorizing such surveillance, 50 U.S.C. § 1804; creates a special court, the Foreign Intelligence Surveillance Court, to pass upon and grant such applications, 50 U.S.C. §§ 1803, 1805; and provides for civil and criminal liability for specified statutory violations, 50 U.S.C. §§ 1809, 1810.

²³ For example, in *City of Milwaukee*, 451 U.S. 304— a case involving an elaborate federal statutory system for dealing with the problem of interstate water pollution under the Federal Water Pollution Control Act—(cont'd)

Case3:08-cv-04373-JSW Document102 Filed09/12/12 Page47 of 62

was intended to govern the use of electronic surveillance in a comprehensive fashion, but whether the FISA speaks clearly and directly to the particular aspect of common law at issue in this litigation—whether the Government is precluded from asserting the state secrets privilege to protect intelligence sources and methods, including whether the plaintiffs have been subject to alleged electronic surveillance.

Moreover, contrary to plaintiffs' reasoning, substantive regulation of foreign intelligence gathering does not encompass the regulation of privilege assertions in cases that touch upon that subject area, much less the state secrets privilege. The state secrets privilege has been and may properly be invoked with respect to a wide range of subject matters, including, tort suits, *see United States v. Reynolds*, 345 U.S. 1 (1953); environmental challenges, *see Kasza*, 133 F.3d at 1162; and procurement disputes, *see General Dynamics Corp.*, 131 S. Ct. 1900.²⁴

C. The Text of Subsection 1806(f) Does Not Displace the State Secrets Privilege or Permit Discovery Into Whether A Person Has Been Subject to Alleged Surveillance.

Turning to the specific FISA provision on which plaintiffs rely, subsection 1806(f) does not expressly or even impliedly displace the state secrets privilege. Plaintiffs' contention proceeds from the premise that both subsection 1806(f) and the state secrets privilege "address the same subject matter" – specifically, the circumstances in which "disclosure [of evidence] or an adversary hearing would harm the national security of the United States." Pls. Mem. at 12

the Supreme Court did not hold that the common law was displaced merely because the federal statutory comprehensively regulated the discharge of pollutants into waterways and overflows of sewage systems, but rather because the statute specifically created a federal permit and administrative process that was found to supplant federal common law remedies for the abatement of interstate water pollution. *See* 451 U.S. at 319-24.

Plaintiffs' "comprehensive scheme" argument also relies on a purported link between FISA Section 1810, which authorizes judicial review as to certain violations, and subsection 1806(f) as means to review those claims. See Pls. Mem. at 17. But that theory, which is unsupported generally, has been overtaken by the Ninth Circuit's decision that Section 1810 does not create a cause of action against the United States. *See Al-Haramain*, 2012 WL 3186088, **3-8.

Case3:08-cv-04373-JSW Document102 Filed09/12/12 Page48 of 62

(citing § 1806(f) and *Al-Haramain*, 507 F.3d at 1196).²⁵ That observation is beside the point. The question is not whether the two procedures implicate the same "subject matter" or share "important characteristics in common" but whether the statutory provision clearly operates to supplant the state secrets privilege. Indeed, plaintiffs' further observation that subsection 1806(f) and the state secrets privilege have radically different outcomes, with subsection 1806(f) requiring courts to use national security evidence that the state secrets privilege would exclude, *see* Pls. Mem. at 12, undercuts the notion that Congress meant to effect such a change and underscores the importance of requiring a clear statement on the matter.

Nothing in the text of subsection 1806(f), its legislative history, or applicable case law, indicates that this provision can be invoked by parties seeking to discover in the first instance whether they have been subject to alleged unlawful surveillance and, if so, to then adjudicate the lawfulness of any such surveillance. Subsection 1806(f) is directed at fundamentally different circumstances: to determine the lawfulness of acknowledged surveillance in proceedings where surveillance evidence is *used* against an "aggrieved" person, that is, against "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).

Subsection 1806(f), entitled "In camera and ex parte review by district court," resides within a section of the FISA that governs the "Use of information" obtained from electronic surveillance conducted pursuant to the FISA. *See* 50 U.S.C. § 1806; *see also Al-Haramain*, 2012 WL 3186088, at * 5. The role that Subsection 1806(f) plays within Section 1806 is crucial to understanding its purpose and function. Subsections (a) to (e) of Section 1806 concern the

Judge Walker's analysis proceeded from a similar observation—that the "procedure described in [sub]section 1806(f), while not identical to the procedure described in *Reynolds*, has important characteristics in common with it—enough, certainly, to establish that it preempts the state secrets privilege as to matters to which it relates." *AHIF*, 564 F. Supp. 2d at 1119. For the reasons set forth herein, that analysis is wrong.

Case3:08-cv-04373-JSW Document102 Filed09/12/12 Page49 of 62

1

2

3

4

5

6

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

disclosure of surveillance information when it is being used by a governmental entity against an aggrieved person.²⁶

Subsection (f) follows and authorizes procedures for the *in camera*, *ex parte* review of information to determine the lawfulness of FISA surveillance in three circumstances involving an aggrieved person: [1] "Whenever a court or other authority is notified pursuant to subsection (c) or (d) of this section" that the Government "intends to enter into evidence or otherwise use or disclose" surveillance-based information in judicial or administrative proceedings against an aggrieved person. See 50 U.S.C. 1806(c), (d), (f); or [2] "[W]henever a motion is made pursuant to subsection (e) of this section" to suppress evidence; or [3] "[W]henever 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." See 50 U.S.C. § 1806(f). When one of these circumstances exists, the Attorney may file an affidavit attesting that "disclosure or an adversary hearing would harm the national security of the United States" and, upon that occasion, subsection 1806(f) authorizes the district court to "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." 50 U.S.C. § 1806(f).

²⁶ The text of section 1806 of the FISA is submitted herewith as Ex. 5. In sum, subsection (a) of Section 1806 requires that information acquired from electronic surveillance conducted pursuant to the FISA be handled in accord with minimization procedures; subsection (b) provides that such information may not be disclosed for law enforcement purposes unless accompanied by a statement that it may only be used in a criminal proceeding with the advance notice of the Attorney General; subsection (c) requires notice by the United States if it intends to use such information against an aggrieved person; subsection (d) imposes a similar notice requirement on states and political subdivisions; and subsection (e) authorizes a motion to suppress such information by a person against whom it is to

be or has been introduced or otherwise used. See 50 U.S.C. § 1806(a)-(e).

Case3:08-cv-04373-JSW Document102 Filed09/12/12 Page50 of 62

The first two circumstances in which the Attorney General may invoke subsection 1806(f) apply where the Government has provided notice of electronic surveillance and affirmatively seeks to use electronic surveillance evidence against an aggrieved person.

Plaintiffs' quotation of subsection 1806(f) omits these two circumstances (*see* Pls. Mem. at 13) and presents only the "motion to discover clause" as if it were a free-standing provision that requires the use of *in camera*, *ex parte* procedures—and thus abrogates the state secrets privilege—whenever a party to a civil action seeks to discover whether they have been subject to alleged electronic surveillance, and, if so, to adjudicate the lawfulness of any such surveillance. But the few words that plaintiffs parse from one sentence in one subsection of Section 1806 cannot bear the meaning ascribed to them, and certainly cannot be said to "speak directly" to displacement of the state secrets privilege.

The Supreme Court has "over and over stressed that '[i]n expounding a statute, [a court] must not be guided by a single sentence or member of a sentence, but [must] look to the provisions of the whole law, and to its object and policy." *Nat'l Bank of Oregon*, 508 U.S. at 455 (1993) (citations omitted). "Statutory construction 'is a holistic endeavor'" that, "at a minimum, must account for" a statute's full text, structure, subject matter, and purpose. *Id*. (citation omitted); *see also Davis v. Michigan Dep't of Treasury*, 489 U.S. 803, 809 (1989)("words of a statute must be read in their context and with a view to their place in the overall statutory scheme.") (citations omitted); *Children's Hosp. Health Ctr. v. Belshe*, 188 F.3d 1090, 1096 (9th Cir. 1999) (same).

Each subsection of Section 1806 governs the use of information acquired through

²⁷ Plaintiffs do not rely on the entire "motion to discover clause" but, through the use of italics and ellipses, omit a reference in this clause to motions to suppress evidence. *See* Pls. Mem. at 13. This omission is significant because, as explained below, the purpose of discovery under subsection 1806(f) is to prepare for a suppression motion.

Case3:08-cv-04373-JSW Document102 Filed09/12/12 Page51 of 62

electronic surveillance, and each provision relates to the disclosure of surveillance information when it is being used by a governmental entity against an aggrieved person.²⁸ The "motion to discover" aspect of subsection 1806(f) fits neatly within the statutory framework governing the use of surveillance evidence against an aggrieved person by addressing circumstances where an aggrieved person as to whom notice of electronic surveillance has been provided may seek discovery in connection with a suppression motion.²⁹

Nothing in Section 1806 indicates that a person can trigger *ex parte, in camera* review by seeking to discover whether he or she has been subject to alleged surveillance. All three circumstances in which subsection 1806(f) applies must involve an "aggrieved person." *See* 50 U.S.C. § 1806(f). The only determination that a district court is authorized to make under subsection 1806(f) is "whether the surveillance of the aggrieved person was lawfully authorized and conducted." 50 U.S.C. § 1806(f). In this case, however, the very question of whether plaintiffs are "aggrieved persons" is subject to the Government's state secrets and statutory privilege assertions, which encompasses any and all "information that would tend to confirm or deny whether the plaintiffs in this action have been subject to" alleged surveillance activities at issue in the complaint. *See* Public DNI Decl. ¶ 22; Public NSA Decl. ¶¶ 16-17. Subsection 1806(f) does not authorize discovery into whether alleged surveillance of a person occurred in

The established canon of *noscitur a sociis* indicates that where "several items in a list shar[e] an attribute," this "counsels in favor of interpreting the other items as possessing that attribute as well"). *See Washington Dep't of Soc. & Health Servs. v. Estate of Keffeler*, 537 U.S. 371, 384-85 (2003); *Adams v. United States*, 420 F.3d 1049, 1053-54 (9th Cir. 2005). Thus the "motions to discover" clause cannot be viewed in isolation but in the same context as other provisions of Section 1806 and 1806(f) that relate to the use of surveillance evidence.

See, e.g., United States v. Warsame, 547 F. Supp. 2d 982, 984-86 (D. Minn. 2008) (defendants brings motion to disclose materials related to FISA surveillance brought after Government provides notice of use of FISA surveillance evidence in order for him to support suppression motion); United States v. Abu-Jihaad, 531 F. Supp. 2d 299, 300-301 (D. Conn. 2008) (same); see also United States v. Damrah, 412 F.2d 618, 622, 623 (6th Cir. 2005) (same). Subsection 1806(g), entitled "suppression of evidence; denial of motion," also links judicial review under subsection 1806(f) to motions to suppress evidence. See 50 U.S.C. § 1806(g).

Case3:08-cv-04373-JSW Document102 Filed09/12/12 Page52 of 62

the first place.³⁰ A contrary interpretation of subsection 1806(f) would transform this provision from a procedure available to the Attorney General to protect national security where surveillance evidence is at issue into a sword that permits a person who merely alleges that surveillance to seek discovery.

D. Legislative History Supports the Conclusion that Subsection 1806(f) Does Not Displace the State Secrets Privilege or Permit Discovery Into Whether Alleged Surveillance Has Occurred.

Legislative history firmly supports the conclusion that subsection 1806(f) applies where the use of surveillance evidence in a proceeding against an aggrieved person is at issue and does not, as the plaintiffs would have it, create a mechanism for persons alleging surveillance to obtain discovery through secure procedures. Congress crafted the provision that became Section 1806 to "set forth *the permissible uses* which may be had of information acquired by means of electronic surveillance conducted pursuant to this chapter." *See* S. Rep. No. 95-701 at 58, 1978 U.S.C.C.A.N. 4027 (Senate Report) (emphasis added). The purpose of these procedures was to strike an "effective balance" between the need for the Government to protect "the secrecy necessary to effective intelligence practices" and "the defendant's constitutional guarantee of a fair trial [that] could be seriously undercut if he is denied the materials needed to prevent a proper defense." *Id.* at 59; 1978 U.S.C.C.A.N. 4028.

The precise reference in subsection 1806(f) to "the surveillance" against "the aggrieved person" (who, again, "is the target" or whose communications "were subject" to electronic surveillance), further indicates that the provision does not concern "alleged" or "possible" surveillance but circumstances where the fact of surveillance is not in dispute in proceedings under subsection 1806(f).

This discussion of legislative history is drawn primarily from the Report of the Senate Select Committee on Intelligence (SSCI) on the Foreign Intelligence Surveillance Act of 1978. See S. Rep. No. 95-701 at 58, 1978 U.S.C.C.A.N. 4027. The Senate Judiciary Committee issued a similar report that includes a nearly verbatim discussion of the provision that became subsection 1806(f). See also S. Rep. No. 95-604, 1978 U.S.C.C.A.N. 3954 (Report of the Senate Committee on the Judiciary). The Senate version of what became subsection 1806(f) was adopted by conference committee reconciling the House and Senate versions of the FISA. See H.R. Conf. Rep. No. 95-1720, at 31-32 (1978). (In the Senate version of the bill, "Subsection (e)" became the current subsection 1806(f). See S. Rep. 95-701 at 63, 1978 U.S.C.C.A.N. 4032)). (cont'd)

Case3:08-cv-04373-JSW Document102 Filed09/12/12 Page53 of 62

1

2

3

4

5

6

7

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

In particular, the Senate report indicates that the *in camera*, ex parte procedures in subsection 1806(f) were intended to address the requirements of Alderman v. United States, 394 U.S. 165 (1969), by providing a secure process for litigating questions of whether evidence being used against someone has been tainted by unlawful surveillance. See S. Rep. 95-701 at 65, 1978 U.S.C.C.A.N 4034.³² The report noted that *Alderman* had not addressed what procedures would apply to evidence obtained from foreign intelligence electronic surveillance. See S. Rep. 95-701 at 65. Legislating in that area of uncertainty, Congress enacted procedures to implement but also modify the Alderman rule where foreign intelligence surveillance is at issue: instead of requiring mandatory disclosure to allow a defendant to probe the issue of taint, subsection 1806(f) permits the Attorney General to trigger the *in camera*, ex parte procedures of subsection 1806(f) to adjudicate the lawfulness of surveillance and suppression motions without the disclosure of foreign intelligence materials that would harm national security. See 50 U.S.C. §1806(f); see S. Rep. 95-701 at 65, 1978 U.S.C.C.A.N 4034 ("The Committee views the procedures set forth in this subsection as striking a reasonable balance between an entirely in camera proceeding which might adversely affect the defendant's ability to defend himself, and mandatory disclosure, which might occasionally result in the wholesale revelation of sensitive foreign intelligence information.").

Legislative history also undercuts plaintiffs' theory that subsection 1806(f) permits discovery into whether a person has been subjected to alleged surveillance. Tellingly, the Senate

In *Alderman*, the Supreme Court held that a criminal defendant was entitled to the discovery of transcripts of unlawfully intercepted conversations in order to determine if any evidence admitted against him was derived from that unlawful surveillance and thus tainted. *See Alderman*, 394 U.S. at 182. The surveillance at issue in that case had been acknowledged, *see id.*, 394 U.S. at 167-68, 170 n.3, and the ultimate issue in the case was whether the evidence against any petitioner grew out of illegally overheard conversations and violated the Fourth Amendment, *see id.* at 181. The Government argued that records of specified conversations first be submitted to the trial judge for *in camera* inspection for a relevance determination before disclosure to petitioner, who could seek to show that the Government had used tainted evidence to convict him. *Id.* But the Supreme Court rejected this approach in order to protect adversary proceedings in the criminal justice system. *Id.* at 183.

Case3:08-cv-04373-JSW Document102 Filed09/12/12 Page54 of 62

Report contrasts subsection 1806(f) with another provision of the U.S. Code—18 U.S.C. § 3504
— which requires the Government to affirm or deny the existence of surveillance where the
admissibility of evidence is challenged in certain proceedings. ³³ The Senate Report makes clear
that this is not how subsection 1806(f) operates. Rather, the report observes that the "most
common circumstance" in which a suppression motion might be brought pursuant to Section
1806 would be "after a defendant queries the Government under 18 U.S.C. § 3504 and discover
that he has been intercepted by electronic surveillance even before the Government has decided
whether evidence derived from that surveillance will be used in the presentation of its case." Se
S. Rep. No. 95-701 at 63, 1978 U.S.C.C.A.N. 4032. The report explains that subsection 1806(f)
"states in detail the procedure the court should follow when it receives a notification under
subsection (c) or a suppression motion is filed under [now subsection 1806(e)]" or "for example
whenever an individual makes a motion pursuant to subsection [(e)] or 18 U.S.C. 3504, or any
other statute or rule of the United States to discover, obtain, or suppress evidence or information
obtained or derived from electronic surveillance conducted pursuant to" the FISA. <i>Id.</i> This
discussion indicates that subsection 1806(f) is not a mechanism for forcing the Government to
confirm or deny alleged surveillance upon a motion to discover but, rather, applies only after a
person has separately determined (either from notice by the Government or through a Section
3504 proceeding) that electronic surveillance has occurred and it is already been established that
the person is "aggrieved" as defined by FISA. Congress was certainly well aware of the

³³ Section 3504 of Title 18, entitled "Litigation concerning the sources of evidence," applies only "upon a claim by a party aggrieved that evidence is inadmissible." 18 U.S.C. § 3504(a)-(c). This provision applies where a person seeks to exclude the use of evidence based on alleged surveillance (typically in grand jury settings). *See Gelbard v. United States*, 408 U.S. 41, 54 (1972); *Bacon v. United States*, 466 F.2d 1196, 1197 (9th Cir. 1972); *In re Grand Jury Investigation (Doe)*, 437 F.3d 855, 858 (9th Cir. 2006) ("A grand jury witness may refuse to answer questions based on illegal interception of his communication.").

Case3:08-cv-04373-JSW Document102 Filed09/12/12 Page55 of 62

procedure in Section 3504 and declined to insert a similar process into subsection 1806(f).³⁴

Further negating plaintiffs' displacement theory, legislative history also makes clear that the procedures set forth in subsection 1806(f) were not intended to compel the Government to disclose intelligence sources and methods related to electronic surveillance that it wished to protect. The Senate Report acknowledges that cases may arise where a court applying subsection 1806(f) may believe that disclosure to the aggrieved person is necessary to make an accurate determination of legality, but the Government argues would harm national security. In that circumstance, even after triggering the *in camera*, *ex parte* review procedures of subsection 1806(f), Congress gave the Government a choice: "either disclose the material or forgo the use of the surveillance-based evidence." *See* S. Rep. No. 95-701 at 65; 1978 U.S.C.C.A.N 4034. ³⁵ By granting the United States the choice to use evidence or dismiss a prosecution, Congress recognized that whether to reveal surveillance information is a matter within the Executive's discretion and is a separate and distinct consideration from the procedures that would apply under subsection 1806(f) should the Government choose to use such evidence. *See also*

³⁴ In entering judgment against the Government in *Al-Haramain*, Judge Walker erroneously applied Section 3504 to shift the burden to the Government to disprove the existence of alleged surveillance where the use of evidence was not at issue. *See In re National Security Agency Telecommunications Records Litigation (Al-Haramain Islamic Foundation, Inc. v. Obama)*, 700 F. Supp. 2d 1182, 1190, 1194 (N.D. Cal. 2010) (citing *United States v. Alter*, 482 F.2d 1016 (9th Cir.1973)). *Alter* itself makes clear that, where a grand jury witness declined to answer questions, the Government would have to confirm or deny alleged surveillance only if a prima facie case was made that surveillance evidence was being used in the "in connection with the grand jury proceeding in which the witness is involved." *Id.* at 1026; *see also In re Grand Jury Witness (Whitnack)*, 544 F.2d 1245, 1247 (9th Cir. 1976) (Kennedy, C.J., concurring) (government has no duty to affirm or deny surveillance under section 3504 where grand inquiry is based on independent evidence); *see also In re Grand Jury Investigation*, 437 F.3d 855, 858-859 (9th Cir. 2006) (same).

The legislative history also explains that the phrase "notwithstanding any other law" in subsection 1806(f) was intended to prevent an "inventive litigant" from bypassing the carefully drawn procedures in subsection 1806(f) by seeking to bring a motion "pursuant to any other statute or rule of the United States." *See* S. Rep. No. 95-701, at 63; S. Rep. No. 96-604, at 57. Accordingly, through this phrase, Congress did not seek to restrict the Government from protecting intelligence sources and methods through a privilege assertion, as plaintiffs' contend, but to restrict litigants from seeking to circumvent subsection 1806(f) by filing motions for discovery under different authority.

Case3:08-cv-04373-JSW Document102 Filed09/12/12 Page56 of 62

1

2

3

4

5

6

7

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

Alderman, 394 U.S. at 181-82, 184 (government had the option to disclose surveillance evidence or dismiss the case).³⁶

Finally, if another indication of Congressional intent were needed, it is noteworthy that when Congress last revisited the FISA to enact comprehensive amendments in 2008—as well as specific procedures to foreclose plaintiffs in this case from bringing a cause of action against telecommunications carriers in the *Hepting* litigation—the Senate Select Committee on Intelligence specifically recognized that the Government asserted the state secrets privilege in the cases against the carriers. See S. Rep. No. 110-209 (110th Cong., 1ST Sess. 2007), 2007 WL 5334390, at 5-6, 9); see also Hepting, 671 F.3d 881, 893 ("The Committee pointed to the pending suits, including this one, noting that "even if these suits are ultimately dismissed on state secrets or some other grounds, litigation is likely to be protracted.") (citing S. Rep. 110-209). The SSCI also noted that the state secrets privilege prevented carriers that could have availed themselves of a defense that they had not assisted the Government, or were entitled to immunity under existing statutory provisions, from taking advantage of such defenses and enacted the new immunity procedures partially to address this situation. *Id.* at 9. It would have made little sense for Congress to have taken this action if it believed that the state secrets privilege was unavailable to the Government in the first instance because FISA displaced it.

E. Judicial Authority Supports the Conclusion that Subsection 1806(f) Does Not Displace the State Secrets Privilege or Permit Discovery Into Whether Alleged Surveillance Has Occurred.

Judicial authority also weighs against plaintiffs' theory that FISA displaces the state secrets privilege and can be used to seek discovery into whether alleged electronic surveillance

³⁶ Reynolds itself contrasted the use of the state secrets privilege in civil litigation with "cases in the criminal field, where it has been held that the Government can invoke its evidentiary privileges only at the price of letting the defendant go free." See Reynolds, 345 U.S. at 12. But Reynolds rejected this very approach in civil litigation where the privilege applies, noting that the rationale in criminal cases "has no application in a civil forum where the Government is not the moving party, but is a defendant only on terms to which it has consented." Id.

Case3:08-cv-04373-JSW Document102 Filed09/12/12 Page57 of 62

1

2

3

4

5

6

7

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

has occurred. Subsection 1806(f) has been consistently applied only where the Government has sought to use evidence related to surveillance in judicial proceedings and invoked 1806(f) to protect against the unauthorized disclosure of FISA applications, orders and related information.³⁷ Courts have recognized that, outside of circumstances where the use of surveillance evidence is at issue, the Government is not required to give notice that alleged electronic surveillance has occurred. For example, in rejecting a Fourth Amendment challenge to provisions of the FISA, as amended by the Patriot Act, Pub.L.No. 107-56, 115 Stat. 272 (Oct. 26, 2001), the Foreign Intelligence Surveillance Court of Review noted that "FISA does not require notice to a person whose communications were intercepted unless the government 'intends to enter into evidence or otherwise use or disclose' such communications in a trial or other enumerated official proceedings." *In re Sealed Case*, 310 F.3d 717, 741 (For. Intel. Surv. Rev. 2002). "[W]here such evidence is not ultimately going to be used for law enforcement, Congress observed that '[t]he need to preserve secrecy for sensitive counterintelligence sources and methods justifies elimination of the notice requirement" that applies to Title III surveillance authority. *Id.* (quoting Sen. Rept. 95-701 at 12, 1978 U.S.C.C.A.N 3980).

Two related cases in the Ninth Circuit and D.C. Circuit further indicate that the FISA is not a tool that permits discovery into whether surveillance has occurred. In *United States v. Hamide*, 914 F.2d 1147 (9th Cir. 1990), which involved a deportation action against eight aliens before the Immigration and Naturalization Service, the Government had acknowledged that it had undertaken FISA surveillance on some of the aliens in response to a motion under 18 U.S.C.

³⁷ See, e.g., United States v. Ott, 827 F.2d 473, 474 (9th Cir. 1987) (subsection 1806(f) applied where Government informed defendant it intended to introduce certain evidence obtained from FISA surveillance); see also United States v. Damrah, 412 F.3d 618, 622 (6th Cir. 2005) (subsection 1806(f) applied where Government admitted audio tapes of FISA surveillance during trial); United States v. Johnson, 952 F.2d 565, 571-73 (1st Cir. 1992) (same); United States v. Duggan, 743 F.2d 59 (2nd Cir. 1984) (Government provided notice of use of surveillance evidence under subsection 1806(c) and subsection 1806(f) applied in response to motion to suppress).

Case3:08-cv-04373-JSW Document102 Filed09/12/12 Page58 of 62

1

2

3

4

5

6

7

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

§ 3504. Subsection 1806(f) of the FISA was then invoked by the Attorney General to determine the lawfulness of that surveillance, which was found to be lawful. *See Hamide*, 914 F.2d at 1148-50.

In contrast, in a separate lawsuit seeking declaratory and injunctive relief brought by the same individuals whose surveillance was at issue in *Hamide*, the D.C. Circuit recognized that, as to those plaintiffs whom the Government had not previously acknowledged surveillance in the Hamide matter, the Government was not required by the FISA to reveal the existence of surveillance. ACLU Foundation v. Barr, 952 F.2d 457 (D.C. Cir. 1991). The court in Barr noted that "if the government is forced to admit or deny such allegations, in an answer to the complaint or otherwise, it will have disclosed sensitive information that may compromise critical foreign intelligence activities." *Id.* at 469; see also id. n.13 ("The government makes the point, with which we agree, that under FISA it has no duty to reveal ongoing foreign intelligence surveillance."). The court in *Barr* declined to uphold dismissal for failure to state a claim under Rule 12(b)(6), but held that, in a Rule 56 summary judgment proceeding, "the government would need only assert that plaintiffs do not have sufficient evidence to carry their burden of proving ongoing surveillance " Barr, 952 F.2d at 469. If the plaintiffs were unable to come forward with such evidence, summary judgment would be entered for the Government . Id. This is the precise scenario of this case: on summary judgment, the Government has asserted the state secrets privilege, which forecloses plaintiffs' ability to establish their standing, and FISA is not a mechanism to defeat that motion.³⁹

³⁸ As to those plaintiffs whose surveillance had been acknowledged, the court in *Barr* held that the Ninth Circuit's decision in *Hamide* adjudicating the lawfulness of the FISA surveillance under subsection 1806(f) foreclosed any further claim. *Barr*, 952 F.2d at 464-65.

The court in *Barr* also observed that subsection 1806(f) would protect against the disclosure of surveillance materials even if a plaintiff could defeat summary judgment, *see Barr*, 952 F.2d at 469, but rejected the (cont'd)

Case3:08-cv-04373-JSW Document102 Filed09/12/12 Page59 of 62

Other than Judge Walker's now-vacated judgment, plaintiffs cannot cite a single instance in which subsection 1806(f) was relied upon to displace the privilege, let alone permit discovery into alleged surveillance. Where plaintiffs must establish that Congress clearly and directly intended to displace the privilege through the FISA, nothing in the statute, legislative history, or case law supports that conclusion.

F. Application of Subsection 1806(f) in this Case Would Itself Risk Disclosure of Properly Protected Information.

A final reason that subsection 1806(f) should not be construed to preempt the state secrets privilege warrants particular emphasis: any attempt to do so would itself risk disclosures that could result in exceptional damage to national security. Far from serving the same purpose as the state secrets privilege, application of subsection 1806(f) in this case would risk the very harms the privilege is intended to prevent. That is because, unlike in circumstances where subsection 1806(f) properly applies—where the existence of surveillance is acknowledged and the use of evidence against an aggrieved person is at issue—here the Government seeks to protect the very question of whether plaintiffs are aggrieved, and whether certain electronic surveillance activities have occurred.

Any effort to establish whether plaintiffs are in fact aggrieved and proceed on the merits under subsection 1806(f) would inherently risk or require the disclosure of properly privileged information—notwithstanding the *in camera* and *ex parte* procedures of that provision. If none of the plaintiffs are aggrieved parties, the case could not proceed, but such a holding would reveal information that is properly protected by the state secrets privilege—namely, that certain

notion these procedures were themselves the mechanism for defeating summary judgment or that they displaced the Government's right to not to reveal whether surveillance had occurred. The court observed that "[s]uits for injunctions against ongoing FISA surveillance . . . are not motions to 'discover or obtain' materials relating to or derived from FISA surveillance," and that subsection 1806(f) does not itself "create or recognize a cause of action for an injunction or for a declaratory judgment, but the scheme it sets up makes clear that nothing in the FISA can be read to create such a cause of action." *Id.* at 470.

Case3:08-cv-04373-JSW Document102 Filed09/12/12 Page60 of 62

individuals were not subject to alleged surveillance. Conversely, if the case did proceed, it could do so only as to an aggrieved party, which would confirm that a particular plaintiff was subject to surveillance. Similarly, assuming there were an aggrieved party in this case, at some point the Court would have to grant or deny relief. If an aggrieved plaintiff were to lose on the merits, only that plaintiff could appeal—and that fact would be disclosed or become apparent in further proceedings. Likewise, if the government were to lose on the merits under subsection 1806(f) as to a particular aggrieved plaintiff, that too would either have to be disclosed or would become apparent upon any appeal. Also, in a case that specifically concerns whether certain alleged activities even occurred, any further proceedings on the merits would not only establish that a plaintiff was aggrieved, but that an alleged activity existed to some extent, thus indirectly and inherently revealing information that the Government seeks to protect through the privilege assertion.

Accordingly, as a replacement for the state secrets privilege, application of the procedures in subsection 1806(f) would be inimical to the proper application of the privilege. As outlined above, the privilege addresses circumstances where risk of disclosure of information in litigation reasonably could be expected to cause damage national security. *See Jeppesen*, 614 F. 3d at 1079; *Kasza*, 133 F.3d at 1167-68. Indeed, *in camera, ex parte* review is not required under the privilege, as "examination of the evidence, even by the judge alone, in chambers," may present too great a risk to national security. *Reynolds*, 345 U.S. at 10. Moreover, an assertion of privilege does not lead to or result in a ruling on the merits based on the consideration of the privileged evidence. Rather, when upheld, the privilege is absolute and the privileged

⁴⁰ See also Al-Haramain v. Bush, 507 F.3d at 1203 ("[w]e acknowledge the need to defer to the Executive on matters of foreign policy and national security and surely cannot legitimately find ourselves second guessing the Executive in this arena").

Case3:08-cv-04373-JSW Document102 Filed09/12/12 Page61 of 62

information at issue is excluded from the case regardless of any showing of need for that information. *Kasza*, 133 F.3d at 1166 (citing *Reynolds*, 345 U.S. at 11). Upon the exclusion of privileged information, the case must either proceed without that information or be dismissed if either the plaintiff cannot prove the *prima facie* elements of her claim without the privileged evidence, or the privilege deprives the defendant of information that would otherwise give the defendant a valid defense to the claim, or the risk of disclosure of the privileged evidence is so great that the protection of national security considerations warrants dismissal. *See Jeppesen*, 614 F.3d at 1083; *Kasza*, 133 F.3d at 1166.

Thus, subsection 1806(f) and the state secrets privilege apply to entirely different circumstances. Where the very existence of alleged surveillance activities is at issue, along with whether plaintiffs have been subject to electronic surveillance, attempting to use subsection 1806(f) procedures out of their appropriate role would risk the very harms to national security that the state secrets privilege is designed to prevent. Courts are not required to "play with fire and chance further disclosure— inadvertent, mistaken, or even intentional—that would defeat the very purpose for which the privilege exists." *Sterling v. Tenet*, 416 F.3d 338, 344 (4th Cir. 2005), *see also Tenet*, 544 U.S. at 11 (rejecting Ninth Circuit's holding that "*in camera* proceedings" were available to adjudicate underlying claims because of the risk of jeopardizing state secrets). Any finding that the FISA displaces the Executive branch's ability to protect highly sensitive intelligence sources and methods in this litigation would be wholly in error.

CONCLUSION

For the foregoing reasons, the Government Defendants Motion to Dismiss and for Summary Judgment should be granted; plaintiffs' motion for partial summary judgment should be denied; and plaintiffs' complaint should be dismissed.

Case3:08-cv-04373-JSW Document102 Filed09/12/12 Page62 of 62

1	September 12, 2012	Respectfully Submitted,
2		STUART F. DELERY
3		Acting Assistant Attorney General
4		JOSEPH H. HUNT
		Director, Federal Programs Branch
5		VINCENT M. GARVEY
6		Deputy Branch Director
7		s/ Anthony J. Coppolino
8		ANTHONY J. COPPOLINO
9		Special Litigation Counsel tony.coppolino@usdoj.gov
10		<u>s/ Marcia Berman</u> MARCIA BERMAN
11		Senior Trial Counsel
12		marcia.berman@usdoj.gov
13		U.S. Department of Justice
14		Civil Division, Federal Programs Branch
		20 Massachusetts Avenue, NW, Rm. 6102 Washington, D.C. 20001
15		Phone: (202) 514-4782
16		Fax: (202) 616-8460
17		Attorneys for the Government Defendants
18		Sued in their Official Capacities
19		
20		
21		
22		
23		
24		
25		
26		
27		
28		