

1 BETH S. BRINKMANN
 Deputy Assistant Attorney General
 2 DOUGLAS N. LETTER
 Terrorism Litigation Counsel
 3 JOSEPH H. HUNT
 Director, Federal Programs Branch
 4 VINCENT M. GARVEY
 Deputy Branch Director
 5 ANTHONY J. COPPOLINO
 Special Litigation Counsel
 6 MARCIA BERMAN
 Senior Trial Counsel
 7 PAUL E. AHERN
 Trial Attorney
 8 U.S. Department of Justice
 Civil Division, Federal Programs Branch
 9 20 Massachusetts Avenue, N.W.
 Washington, D.C. 20001
 10 Phone: (202) 514-4782
 Fax: (202) 616-8460

11 *Attorneys for the Government Defendants*

12
 13 **UNITED STATES DISTRICT COURT**
 14 **NORTHERN DISTRICT OF CALIFORNIA**
 15 **SAN FRANCISCO DIVISION**

16)	No. M:06-cv-01791-VRW
17)	GOVERNMENT DEFENDANTS'
18)	NOTICE OF RENEWED MOTION TO
19)	DISMISS AND FOR SUMMARY
20)	JUDGMENT AND MEMORANDUM
21)	IN SUPPORT
<hr/>		
22)	Date: December 15, 2009
23)	Time: 10:00 a.m.
24)	Courtroom: 6, 17 th Floor
25)	Chief Judge Vaughn R. Walker

26 PLEASE TAKE NOTICE that on December 15, 2009, at 10:00 a.m., in Courtroom 6, 17th
 27 Floor, before Chief Judge Vaughn R. Walker, the Government Defendants sued in their official
 28 capacity (the United States of America; Barack Obama, President of the United States; Keith B.
 Alexander, Director of the National Security Agency; and Eric Holder, Attorney General of the

1 United States)¹ will move to dismiss certain claims in the plaintiffs' Amended Complaint
2 pursuant to Rule 12(b)(1) of the Federal Rules of Civil Procedure, and will seek summary
3 judgment as to any remaining claims pursuant to Rule 56 of the Federal Rules of Civil
4 Procedure.²

5 The grounds for these motions are as follows: (1) plaintiffs' statutory claims against the
6 United States and Government Defendants sued in their official capacity, brought pursuant to 50
7 U.S.C. § 1810, 18 U.S.C. § 2520, and 18 U.S.C. § 2707(c) (*see* Dkt. 284 in MDL 06-cv-1791-
8 VRW), should be dismissed for lack of subject matter jurisdiction pursuant to Rule 12(b)(1) of
9 the Federal Rules of Civil Procedure on the ground that Congress has not waived the sovereign
10 immunity of the United States for any claim for relief pursuant to these statutory causes of action;
11 and (2) summary judgment should be entered for the United States and the Government
12 Defendants sued in their official capacity with respect to all of plaintiffs' claims against all
13 defendants (including any statutory claim against the Government Defendants not otherwise
14 dismissed for lack of jurisdiction and any claim against any personal capacity defendant) on the
15 ground that information necessary to litigate all of plaintiffs' claims against all defendants is
16 properly subject to, and excluded from use in this case by, the state secrets privilege and related
17 statutory privileges raised by the Director of National Intelligence and the Director of the
18 National Security Agency.

19 The grounds for this motion are set forth further in the accompanying (i) Memorandum of
20 Points and Authorities in Support of the Government Defendants' Motion to Dismiss and for
21

22 ¹ Pursuant to Rule 25(d) of the Federal Rules of Civil Procedure, President Obama and
23 Attorney General Holder are substituted in their official capacities as defendants.

24 ² On May 25, 2007, the Government Defendants filed a motion seeking dismissal or
25 summary judgment in their favor based on the Government's assertion of the state secrets and related
26 statutory privileges. (*See* Dkt. 295 in MDL 06-cv-1791-VRW). By Order dated March 31, 2008,
27 the Court administratively terminated the Government's motion after the U.S. Court of Appeals for
28 the Ninth Circuit withdrew from submission a pending appeal in *Hepting v. AT&T*, 439 F. Supp. 2d
974 (N.D. Cal. 2006), but granted the Government leave to "petition the court to reopen these
motions if the circumstances warrant." (*See* Dkt. 438 in MDL 06-cv-1791-VRW). After a case
management conference on September 9, 2009, the Court granted the Government leave to renew
its dispositive motions in this action. (*See* Dkt. 31).

1 Summary Judgment; (ii) Ex.1, Public Declaration of Dennis C. Blair, Director of National
2 Intelligence (hereafter “Public DNI Decl.”); and (iii) Ex.2, Public Declaration of Lieutenant
3 General Keith B. Alexander, Director, National Security Agency (hereafter “Public NSA Decl.”).
4 Additional grounds for these motions are also set forth in the (iv) Classified Declaration of
5 Dennis C. Blair, Director of National Intelligence; (v) Classified Declaration of Lieutenant
6 General Keith B. Alexander, Director, National Security Agency; and (vi) Supplemental
7 Classified Memorandum of Points and Authorities in Support of the Government Defendants’
8 Motion to Dismiss and for Summary Judgment. These classified materials have been lodged
9 with court security officers and are available upon request solely for the Court’s *in camera* and *ex*
10 *parte* review.

11 Date: October 30, 2009

Respectfully Submitted,

BETH S. BRINKMANN
Deputy Assistant Attorney General

DOUGLAS N. LETTER
Terrorism Litigation Counsel

JOSEPH H. HUNT
Director, Federal Programs Branch

VINCENT M. GARVEY
Deputy Branch Director

s/ Anthony J. Coppolino
ANTHONY J. COPPOLINO
Special Litigation Counsel

s/ Marcia Berman
MARCIA BERMAN
Senior Trial Counsel

s/ Paul E. Ahern
PAUL E. AHERN
Trial Attorney

U.S. Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Avenue, NW, Rm. 6102
Washington, D.C. 20001
Phone: (202) 514-4782
Fax: (202) 616-8460
Email: tony.coppolino@usdoj.gov

Attorneys for the Government Defendants

1 BETH S. BRINKMANN
 2 Deputy Assistant Attorney General
 DOUGLAS N. LETTER
 3 Terrorism Litigation Counsel
 JOSEPH H. HUNT
 4 Director, Federal Programs Branch
 VINCENT M. GARVEY
 5 Deputy Branch Director
 ANTHONY J. COPPOLINO
 6 Special Litigation Counsel
 MARCIA BERMAN
 7 Senior Trial Counsel
 PAUL E. AHERN
 8 Trial Attorney
 U.S. Department of Justice
 9 Civil Division, Federal Programs Branch
 20 Massachusetts Avenue, N.W.
 10 Washington, D.C. 20001
 Phone: (202) 514-4782
 11 Fax: (202) 616-8460

12 *Attorneys for the Government Defendants*

13 **UNITED STATES DISTRICT COURT**
 14 **NORTHERN DISTRICT OF CALIFORNIA**
 15 **SAN FRANCISCO DIVISION**

16 IN RE NATIONAL SECURITY AGENCY)
 17 TELECOMMUNICATIONS RECORDS)
 18 LITIGATION)
 19 _____)
 20 This Document Relates Solely To:)
 21 *Shubert et al. v. United States of America et al.*)
 (Case No. 07-cv-00693-VRW))
 22 _____)

No. M:06-cv-01791-VRW
**GOVERNMENT DEFENDANTS’
 MEMORANDUM IN SUPPORT OF
 RENEWED MOTION TO DISMISS
 AND FOR SUMMARY JUDGMENT**

Date: December 15, 2009
 Time: 10:00 a.m.
 Courtroom: 6, 17th Floor
 Chief Judge Vaughn R. Walker

22
 23
 24
 25
 26
 27
 28

TABLE OF CONTENTS

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

INTRODUCTION..... 1

ARGUMENT..... 3

 I. PLAINTIFFS’ STATUTORY CLAIMS SHOULD BE DISMISSED
 FOR LACK OF JURISDICTION. 3

 II. INFORMATION SUBJECT TO THE GOVERNMENT’S STATE
 SECRETS PRIVILEGE ASSERTION (AND RELATED
 STATUTORY PRIVILEGE ASSERTIONS) SHOULD BE
 EXCLUDED FROM THIS CASE..... 4

 A. The State Secrets Privilege Bars the Use of Privileged
 Information in Litigation. 5

 B. The United States has Properly Asserted the State
 Secrets Privilege Here. 7

 C. The DNI and NSA Director Have Properly Raised Statutory
 Privileges to Exclude Information Concerning Intelligence
 Sources and Methods From This Case..... 9

 III. SUMMARY JUDGMENT SHOULD BE ENTERED FOR THE
 GOVERNMENT BECAUSE THE EVIDENCE NEEDED
 TO LITIGATE PLAINTIFFS’ STANDING AND CLAIMS
 ON THE MERITS IS PROPERLY EXCLUDED BY THE
 STATE SECRETS AND RELATED STATUTORY PRIVILEGES. 10

 A. Plaintiffs Cannot Establish Their Standing Without
 the Disclosure of Information Subject to the DNI’s
 Privilege Assertion..... 12

 B. The Disclosure of Privileged Information Would
 Also Be At Risk or Required to Adjudicate
 Plaintiffs’ Claims on the Merits..... 15

 IV. LITIGATION OF THE PLAINTIFFS’ CLAIMS CANNOT
 PROCEED UNDER THE FISA. 22

CONCLUSION..... 23

TABLE OF AUTHORITIES

CASES

1

2

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

4 *Al-Haramain Islamic Found., Inc. v. Bush*, 564 F. Supp. 2d 1109 (N.D. Cal. 2008). 4, 6

5 *Am. Civil Liberties Union v. NSA*, 493 F.3d 644 (6th Cir. 2007). 13

6 *Amnesty Int’l v. McConnell*, —F. Supp. 2d—, 2009 WL 2569138 (S.D.N.Y. 2009). 13

7 *Bareford v. General Dynamics Corp.*, 973 F.2d 1138 (5th Cir. 1992). 11, 13

8 *CIA v. Sims*, 471 U.S. 159 (1985). 6, 12, 18

9 *City of Los Angeles v. Lyons*, 461 U.S. 95 (1983). 12

10 *Dep’t of the Army v. Blue Fox, Inc.*, 525 U.S. 255 (1999). 3

11 *Dept. of the Navy v. Egan*, 484 U.S. 518 (1988). 5

12 *El-Masri v. United States*, 479 F.3d 296 (4th Cir. 2007). 5

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

14 *Farnsworth Cannon, Inc. v. Grimes*, 635 F.2d 268 (4th Cir. 1980). 20

15 *F.D.I.C. v. Meyer*, 510 U.S. 471 (1994). 3

16 *Fitzgerald v. Penthouse Int’l Ltd.*, 776 F.2d 1236 (4th Cir. 1985). 20

17 *Frost v. Perry (Frost I)*, 161 F.R.D. 434 (D. Nev. 1995). 21-22

18 *Frost v. Perry (Frost II)*, 919 F. Supp. 1459 (D. Nev. 1996). 21-22

19 *Halkin v. Helms (Halkin I)*, 598 F.2d 1 (D.C. Cir. 1978). 6, 13

20 *Halkin v. Helms (Halkin II)*, 690 F.2d 977 (D.C. Cir. 1982). 5, 8, 13

21 *Hepting v. AT&T*, 439 F. Supp. 2d 974 (N.D. Cal. 2006). *passim*

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

23 *Lane v. Pena*, 518 U.S. 187 (1996). 3

24 *Lewis v. Casey*, 518 U.S. 343 (1996) 12

25 *Lujan v. Defenders of Wildlife*, 504 U.S. 555 (1992). 12

26 *Mohamed v. Jeppesen Dataplan, Inc.*, 579 F.3d 943 (9th Cir. amended Aug. 31, 2009). 18, 22

27 *New Jersey v. T.L.O.*, 469 U.S. 325 (1985). 17

28 *O’Connor v. Ortega*, 480 U.S. 709 (1987). 17

1 *People for the American Way Found v. NSA (PFAW)*, 462 F. Supp. 2d 21 (D.D.C. 2006). . . 10, 13
 2 *Prescott v. United States*, 973 F.2d 696 (9th Cir. 1992). 3
 3 *Rakas v. Illinois*, 439 U.S. 128 (1978) 14
 4 *Sigman v. United States*, 217 F.3d 785 (9th Cir. 2000). 3
 5 *Smith v. Maryland*, 442 U.S. 735 (1979). 17
 6 *Tenet v. Doe*, 544 U.S. 1 (2005). 18
 7 *Terkel v. AT&T Corp.*, 441 F. Supp. 2d 899 (N.D. Ill. 2006). 12-13, 15, 18
 8 *Totten v. United States*, 92 U.S. 105 (1875). 5, 18
 9 *United States v. Burr*, 25 F. Cas. 30 (C.C.D. Va. 1807). 5
 10 *United States v. Forrester*, 512 F.3d 500 (9th Cir. 2007). 17
 11 *United States v. Marchetti*, 466 F.2d 1309 (4th Cir. 1972). 6
 12 *United States v. Nixon*, 418 U.S. 683 (1974). 5
 13 *United States v. Nordic Village, Inc.*, 503 U.S. 30 (1992). 3
 14 *United States v. Reynolds*, 345 U.S. 1 (1953). *passim*
 15 *Warth v. Seldin*, 422 U.S. 490 (1975). 12
 16 *Wilner v. NSA*, No. 07 Civ. 3883, 2008 WL 2567765 (S.D. N.Y. June 25, 2008). 10, 13
 17 *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579 (1952). 9
 18 *Zuckerbraun v. General Dynamics Corp.*, 935 F.2d 544 (2d Cir. 1991). 11, 19

19 **CONSTITUTIONAL PROVISIONS**

20 U.S. CONST. amend. IV. 2-3, 8, 17

21 **STATUTES**

22 18 U.S.C. § 2510. 8, 13, 16
 23 18 U.S.C. § 2511. 16
 24 18 U.S.C. § 2520. 2-3, 14
 25 18 U.S.C. § 2675. 3
 26 18 U.S.C. § 2701. 8, 16
 27 18 U.S.C. § 2703. 8
 28 18 U.S.C. § 2707. 2-3, 14

1 18 U.S.C. § 2711. 14
 2 18 U.S.C. § 2712. 3-4
 3 50 U.S.C. § 402 note. 10
 4 50 U.S.C. § 403. 7
 5 50 U.S.C. § 403-1. 10
 6 50 U.S.C. § 1801. 16
 7 50 U.S.C. § 1806. 22-23
 8 50 U.S.C. § 1809. 16
 9 50 U.S.C. § 1810. 2-4, 13

10 **LEGISLATIVE MATERIALS**

11 S. REP. NO. 110-209 (2007). 18
 12 H.R. REP. NO. 95-1283 (1978). 14

13 **RULES**

14 Fed. R. Civ. P. 12. 2
 15 Fed. R. Civ. P. 56. 2, 20
 16 Ninth Cir. R. 35-3. 18
 17 Ninth Cir. Gen. Order 5.5. 18

18
 19
 20
 21
 22
 23
 24
 25
 26
 27
 28

INTRODUCTION

1
2 Plaintiffs in this action allege that the National Security Agency (“NSA”), pursuant to a
3 presidential authorization after the terrorist attacks of September 11, 2001, has engaged in an
4 alleged “dragnet” of warrantless surveillance that targets “virtually every telephone, internet
5 and/or email communication that has been sent from or received within the United States since
6 2001”—a “secret program to spy upon millions of innocent Americans.” Amended Complaint
7 ¶¶ 1-4 (Dkt. 284 in MDL 06-cv-1791-VRW) (“Am. Compl.”). Plaintiffs are four individuals
8 who reside in Brooklyn, New York, and their claims are based on allegations made in a
9 December 2005 story in *The New York Times*, as well as on public statements made by then-
10 President Bush. See Am. Compl. ¶ 50. At the time, President Bush indicated that he had
11 authorized the NSA to conduct a surveillance program (subsequently referred to as the Terrorist
12 Surveillance Program or “TSP”) directed at “one-end” international communications to or from
13 the United States as to which reasonable grounds existed to believe that one of the communicants
14 was a member of al-Qaeda or an affiliated group. See *Hepting v. AT&T*, 439 F. Supp. 2d 974,
15 987 (N.D. Cal. 2006).

16 Plaintiffs do not contend that they communicate with individuals who may be members of
17 agents of al-Qaeda and, thus, that they may be subject to TSP surveillance.³ Rather, they posit a
18 highly speculative allegation of a surveillance “dragnet” that goes well beyond the TSP’s
19 acknowledged parameters and allege, *inter alia*, that the NSA monitors the content of “millions”
20 of communications, including purely domestic and international telephone and Internet
21 communications, and then analyzes that information through key word searches. See, e.g., Am.
22 Compl. ¶¶ 59-62. Plaintiffs claim they are personally subject to this alleged dragnet surveillance
23 on the ground that they regularly make phone calls and send emails both within and outside the
24 United States, specifically to the United Kingdom, France, Italy, Egypt, the Netherlands, and
25 Norway. See *id.* ¶¶ 5-8, 87.

26
27
28 ³ As the Government previously advised the Court, the TSP was supplanted by orders of the
Foreign Intelligence Surveillance Court in January 2007 and subsequently was not re-authorized.
(See Dkt. 127 in MDL 06-cv-1791-VRW).

1 Based on these allegations, plaintiffs bring a four-count amended complaint against the
2 United States as well as current (and former) Government officials claiming that the alleged
3 actions violate several statutory provisions, including the Foreign Intelligence Surveillance Act
4 (“FISA”), 50 U.S.C. § 1810, the Wiretap Act, as amended by the Electronic Communications
5 Privacy Act (“ECPA”), 18 U.S.C. § 2520, and the Stored Communication Act (“SCA”), 18
6 U.S.C. § 2707, as well as the Fourth Amendment. *See* Am. Compl. ¶¶ 97-112. Plaintiffs seek
7 declaratory and injunctive relief, as well as damages. *See id.*; *see also id.* at 24.

8 As a threshold matter, pursuant to Rule 12(b)(1) of the Federal Rules of Civil Procedure,
9 the Court should dismiss plaintiffs’ statutory claims against the United States and Government
10 Defendants sued in their official capacity for lack of jurisdiction on the ground that Congress has
11 not waived the sovereign immunity of the United States to authorize claims for relief under the
12 provisions on which plaintiffs rely. But beyond this, plaintiffs’ claims could not proceed in any
13 event because litigation of their allegations would risk or require the disclosure of information
14 that is properly subject to the state secrets privilege and related statutory privileges asserted in
15 this action by the Director of National Intelligence (“DNI”) and the Director of the NSA. This
16 lawsuit squarely puts at issue whether and to what extent the Government has utilized certain
17 intelligence sources and methods after the 9/11 attacks to detect and prevent further terrorist
18 attacks. The “dragnet” allegations made by the *Shubert* plaintiffs are similar to those asserted in
19 *Jewel v. NSA*, No. 09-cv-4373-VRW, and, as in *Jewel*, the DNI and the NSA have again
20 demonstrated that the disclosure of the evidence necessary to address these allegations would
21 cause exceptionally grave harm to national security and, therefore, that the privileged information
22 must be excluded from this case. In addition, because disclosure of the privileged information
23 would be necessary for plaintiffs to establish their standing and to litigate any claim in any
24 further proceedings, the Court should grant summary judgment for the United States and
25 Government Defendants as to all claims against all parties. Fed. R. Civ. P. 56.

ARGUMENT**I. PLAINTIFFS' STATUTORY CLAIMS SHOULD BE DISMISSED FOR LACK OF JURISDICTION.**

Before reaching the Government's state secrets privilege assertion, a threshold jurisdictional issue should be addressed. In addition to bringing a Fourth Amendment challenge, plaintiffs seek damages against the United States under three statutory provisions: the FISA, 50 U.S.C. § 1810, the Wiretap Act, 18 U.S.C. § 2520, and the SCA, 18 U.S.C. § 2707 (Counts I-III). It is axiomatic, however, that "[a]bsent 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 *F.D.I.C. v. Meyer*, 510 U.S. 471, 475 (1994)). The plaintiffs bear the burden of establishing such a waiver, *see Prescott v. United States*, 973 F.2d 696, 701 (9th Cir. 1992), which must be explicitly and unequivocally expressed in statutory text, *see Lane v. Pena*, 518 U.S. 187, 192 (1996); *Sigman v. United States*, 217 F.3d 785, 792 (9th Cir. 2000). This Court must "strictly construe[]" any purported waiver "in favor of the sovereign," *Blue Fox*, 525 U.S. at 261, and a statute does not constitute the necessary explicit waiver of sovereign immunity if it will bear any "plausible" alternative interpretation, *see United States v. Nordic Village, Inc.*, 503 U.S. 30, 33-37 (1992). Here, plaintiffs can establish no waiver of sovereign immunity for their statutory claims.

First, Congress has *expressly* barred suits against the United States for damages and equitable relief under Section 2520 of the Wiretap Act and Section 2707 of the SCA, in both cases by permitting relief against only a "person or entity *other than the United States.*" 18 U.S.C. § 2520(a) (emphasis added); *see* 18 U.S.C. § 2707(a). A waiver of sovereign immunity must be explicit and unequivocal, but in this case the *preservation* of sovereign immunity is absolutely clear, and the plaintiffs' claims under Sections 2520 and 2707 are barred.⁴

⁴ Plaintiffs here do not invoke Title 18, U.S. Code, Section 2712, as the source for any purported waiver of sovereign immunity with respect to claims brought under Sections 2520 and 2707, and that Section requires exhaustion of administrative remedies prior to the commencement of suit. 18 U.S.C. § 2712(b); *id.* § 2675. Unlike the plaintiffs in *Jewel*, plaintiffs do not appear to have fulfilled any of the administrative prerequisites for bringing a claim under Section 2712, *id.* § 2675, and such a claim would therefore be barred even if it had been invoked by plaintiffs. (See Dkt.

(continued...)

1 Second, the Government continues to contend that Section 1810 of the FISA does not
2 waive sovereign immunity to permit damages claims against the United States. We recognize
3 that the Court has found an “[i]mplicit” waiver of sovereign immunity under Section 1810, *see*
4 *Al-Haramain Islamic Found., Inc. v. Bush*, 564 F. Supp. 2d 1109, 1124-25 (N.D. Cal. 2008), and
5 respectfully reserve our position to the contrary in this case. We note again only that Congress
6 expressly authorized actions for damages “against the United States” as to specific violations of
7 the FISA, *see, e.g.*, 18 U.S.C. § 2712—but not as to alleged violations of Section 1810. Without
8 such an express waiver, plaintiffs’ FISA claim, like their other statutory claims, may not
9 proceed.⁵

10 **II. INFORMATION SUBJECT TO THE GOVERNMENT’S STATE SECRETS
11 PRIVILEGE ASSERTION (AND RELATED STATUTORY PRIVILEGE
12 ASSERTIONS) SHOULD BE EXCLUDED FROM THIS CASE.**

13 Apart from the threshold jurisdictional issue outlined above, litigation of plaintiffs’
14 claims (including any claim that survives dismissal under Rule 12) would risk or require
15 disclosure of information properly protected by the state secrets privilege and related statutory
16 privileges. Plaintiffs clearly seek disclosure of whether and to what extent the Government may
17 have used certain intelligence sources and methods after 9/11 to detect and prevent further
18 attacks. Moreover, plaintiffs seek disclosure of whether any of the alleged activities, if they
19 exist, are ongoing. As set forth herein, the Director of National Intelligence, supported by the
20 Director of the NSA, has properly asserted privilege to protect such information from disclosure
21 to prevent exceptionally grave harm to national security, and this information should therefore be
22 excluded from further proceedings.

23
24
25 ⁴(...continued)

26 1 ¶ 19 in No. 08-cv-4373-VRW). In any event, Section 2712 does not provide for a waiver of
27 sovereign immunity either, for reasons described in the Government dispositive motion in the *Jewel*
28 action. (See Dkt. 18 at 3-6 in No. 08-cv-4373-VRW).

⁵ The Government briefed this sovereign immunity issue in the *Al-Haramain* action and
hereby incorporates its prior arguments. (See Dkt. 17 at 8-12 and Dkt. 29 at 4-8 in No. 07-cv-109-
VRW).

A. The State Secrets Privilege Bars the Use of Privileged Information in Litigation.

1
2 “The state secrets privilege is a common law evidentiary privilege that permits the
3 government to bar the disclosure of information if ‘there is a reasonable danger’ that disclosure
4 will ‘expose military matters which, in the interests of national security, should not be
5 divulged.’” *Al-Haramain Islamic Found. v. Bush*, 507 F.3d 1190, 1196 (9th Cir. 2007) (quoting
6 *United States v. Reynolds*, 345 U.S. 1, 10 (1953)). The ability of the Executive to protect state
7 secrets from disclosure in litigation has been recognized from the earliest days of the Republic.
8 *Totten v. United States*, 92 U.S. 105 (1875) (citing the proceedings against Aaron Burr, *United*
9 *States v. Burr*, 25 F. Cas. 30 (C.C.D. Va. 1807)); *see Reynolds*, 345 U.S. at 7-9; *Al-Haramain*,
10 507 F.3d at 1196-97; *Kasza v. Browner*, 133 F.3d 1159, 1165-66 (9th Cir. 1998); *see also*
11 *Hepting*, 439 F. Supp. 2d at 980-81.⁶ The privilege protects a broad range of information, but
12 especially the “disclosure of intelligence-gathering methods or capabilities.” *See Ellsberg v.*
13 *Mitchell*, 709 F.2d 51, 57 (D.C. Cir. 1983) (footnotes omitted); *accord Al-Haramain*, 507 F.3d
14 1202-03 (holding that state secrets privilege precludes disclosure of whether plaintiffs were
15 subject to foreign intelligence surveillance);⁷ *see also Halkin v. Helms (Halkin II)*, 690 F.2d 977,
16 990 (D.C. Cir. 1982) (holding that state secrets privilege protects intelligence source and
17 methods involved in NSA surveillance). The privilege also protects information that on its face
18 may appear innocuous, but which, when placed in a larger context, could reveal sensitive
19 classified information. *Kasza*, 133 F.3d at 1166.

20 An assertion of the state secrets privilege “must be accorded the ‘utmost deference’ and
21

22
23 ⁶ The privilege also has a firm foundation in the President’s authority under Article II of the
24 Constitution to protect national security information. *See Dept. of the Navy v. Egan*, 484 U.S. 518,
25 527 (1988); *see also United States v. Nixon*, 418 U.S. 683, 710-11 (1974) (citing *Reynolds* and
26 recognizing the President’s constitutional authority to protect national security information); *El-*
27 *Masri v. United States*, 479 F.3d 296, 304 (4th Cir. 2007) (citing *Reynolds* and *Nixon*).

28 ⁷ The Government recognizes that the Ninth Circuit remanded the case in *Al-Haramain* for
this Court to consider whether the Foreign Intelligence Surveillance Act preempts the state secrets
privilege, 507 F.3d at 1205-06, and that this Court subsequently ruled that the privilege is so
preempted, *Al-Haramain*, 564 F. Supp. 2d at 1115-125. As set forth below, the Government
expressly preserves its position in this case that the FISA does not preempt the state secrets privilege
or other statutory privileges.

the court's review of the claim of privilege is narrow." *Kasza*, 133 F.3d at 1166; *see also Al-Haramain*, 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."); *see also CIA v. Sims*, 471 U.S. 159, 180 (1985) ("[I]t is the responsibility of the [Director of National Intelligence], not that of the judiciary, to weigh the variety of complex and subtle factors in determining whether disclosure of information may lead to an unacceptable risk of compromising the . . . intelligence-gathering process."); *Halkin v. Helms (Halkin I)*, 598 F.2d 1, 9 (D.C. Cir. 1978) ("[C]ourts, of course, are ill-equipped to become sufficiently steeped in foreign intelligence matters to serve effectively in the review of secrecy classifications in that area.") (quoting *United States v. Marchetti*, 466 F.2d 1309, 1318 (4th Cir. 1972)). Once properly invoked, the sole determination for the court is whether, "under the particular circumstances of the case, 'there is a reasonable danger that compulsion of the evidence will expose military matters which, in the interest of national security, should not be divulged.'" *Kasza*, 133 F.3d at 1166 (quoting *Reynolds*, 345 U.S. at 10).⁸ The focal point of judicial review is whether the Government has identified the harm to national security at stake—not the court's own assessment of whether information is a secret or the harm that would

⁸ Under an administrative policy announced on September 23, 2009, the U.S. Department of Justice will defend an assertion of the state secrets privilege in litigation when a government department or agency seeking to assert the privilege makes a sufficient showing that assertion of the privilege is necessary to protect information the unauthorized disclosure of which reasonably could be expected to cause significant harm to the national security or foreign relations of the United States. *See* Ex.3 § 1.A. In addition, the policy allows invocation of the privilege "only to the extent necessary to protect against the risk of significant harm to national security," and the Department will move "to dismiss a litigant's claim or case on the basis of the state secrets privilege only when doing so is necessary to protect against the risk of significant harm to national security." *Id.* § 1.B. Section 1.C of the Department's policy places further limitations on the Government's defense of a state secrets privilege assertion, for example, by prohibiting such invocations for the purpose of concealing violations of the law or to prevent embarrassment to the Government. *Id.* § 1.C. As set forth below, the DNI's state secrets privilege assertion in this case satisfies the standard of Section 1.A by finding that disclosure of the information at issue here reasonably could be expected to cause not only significant but exceptionally grave harm to the national security of the United States. *See* Public DNI Decl. ¶ 3. The DNI's privilege assertion has been reviewed within the Department of Justice and approved by the Attorney General, pursuant to Sections 3 and 4 of the new Department policy. That review determined that the DNI's assertion satisfied all of the standards required for a defense of the state secrets privilege according to Section 1 of the Attorney General's policy.

1 result from disclosure. *See Al-Haramain*, 507 F.3d at 1203 (“[J]udicial intuition . . . is no
2 substitute for documented risks and threats posed by the potential disclosure of national security
3 information.”).

4 Moreover, in assessing whether to uphold a claim of privilege, the court does not balance
5 the respective needs of the parties for the information. Rather, “[o]nce the privilege is properly
6 invoked and the court is satisfied as to the danger of divulging state secrets, the privilege is
7 absolute” and cannot be overcome by even the most compelling need in the litigation. *Kasza*,
8 133 F.3d at 1166; *see Reynolds*, 345 U.S. at 11 (“[E]ven the most compelling necessity cannot
9 overcome the claim of privilege if the court is ultimately satisfied that military secrets are at
10 stake.”); *see also Ellsberg*, 709 F.2d at 57.

11 **B. The United States Has Properly Asserted the State Secrets Privilege Here.**

12 The United States has properly asserted and supported its invocation of the privilege here.
13 First, “[t]here must be a formal claim of privilege, lodged by the head of the department which
14 has control over the matter, after actual personal consideration by that officer.” *Reynolds*, 345
15 U.S. at 7-8 (footnotes omitted). In this case, the DNI, who is head of the United States
16 Intelligence Community, *see* 50 U.S.C. § 403 (b)(1); *Al-Haramain*, 507 F.3d at 1202 n.6, has
17 formally asserted the state secrets privilege after personal consideration of the matter. *See* Public
18 and Classified *In Camera*, *Ex Parte* Declarations of Dennis C. Blair, Director of National
19 Intelligence.⁹

20 Second, the Court “must determine whether the circumstances are appropriate for the
21 claim of privilege, and yet do so without forcing a disclosure of the very thing the privilege is
22 designed to protect.” *Reynolds*, 345 U.S. at 8 (footnote omitted). Here, the Government has
23 amply demonstrated that there is a reasonable danger that disclosure of the privileged
24 information would cause exceptionally grave harm to national security. Plaintiffs’ allegations
25 implicate several facts at the heart of the Government’s privilege assertion, risking that

26
27 ⁹ Admiral Blair’s assertion of the privilege is supported by the Public and Classified *In*
28 *Camera*, *Ex Parte* Declarations of Lieutenant General Keith B. Alexander, Director of the National
Security Agency. The classified declarations are submitted solely for the Court’s *in camera* and *ex*
parte review.

1 “disclosure of the very thing the privilege is designed to protect.” For example, plaintiffs allege
2 that they have been personally subject to alleged NSA intelligence activities. *See, e.g.,* Am.
3 Compl. ¶¶ 5-8. But the DNI has explained that the disclosure of information concerning whether
4 or not these plaintiffs have been subject to alleged NSA intelligence activity would inherently
5 reveal NSA intelligence sources and methods—the core matters the privilege is designed to
6 protect. *See Ellsberg*, 709 F.2d at 57; *Halkin II*, 690 F.2d at 990. Whether specific individuals
7 were targets of alleged NSA activities would either reveal who is subject to investigative
8 interest—helping that person to evade surveillance—or who is not—thereby revealing the scope
9 of intelligence activities as well as the existence of secure channels for enemies of the United
10 States to shield their communication. *See* Public DNI Decl. ¶ 13; Public NSA Decl. ¶¶ 16-17.

11 Moreover, plaintiffs allege that they have been subject to a dragnet on the content of their
12 communications as part of an alleged presidentially-authorized program after the 9/11 attacks.
13 *See, e.g.,* Am. Compl. ¶ 2. But the facts necessary to litigate these allegations are also properly
14 excluded by the DNI’s privilege assertion. The DNI has explained that, as the Government has
15 previously acknowledged, the NSA’s collection of the content¹⁰ of communications under the
16 now inoperative TSP was directed at international communications in which a participant was
17 reasonably believed to be associated with al-Qaeda or an affiliated terrorist organization, and thus
18 plaintiffs’ allegation that the NSA has indiscriminately collected the content of millions of
19 communications sent or received by people inside the United States after 9/11 under the TSP is
20 false. *See* Public DNI ¶ 15; *see also* Public NSA Decl. ¶ 19. But attempting to demonstrate that
21 the TSP was not the content dragnet plaintiffs allege, or that the NSA has not otherwise engaged
22 in the alleged content dragnet, would require the disclosure of highly classified NSA intelligence
23 sources and methods about the TSP and other NSA activities. *See* Public DNI Decl. ¶ 15; *see*
24 *also* Public NSA Decl. ¶ 19.¹¹

25
26 ¹⁰ The term “content” is used here and by the DNI to refer to the substance, meaning or
27 purport of a communication, as defined in Title 18, U.S. Code, § 2510(8). *See* Public DNI Decl.
28 ¶ 14 n.1.

¹¹ Plaintiffs’ allegations appear to encompass only the alleged interception of the “content”
(continued...)

1 Plaintiffs also assert that the NSA's alleged activities are assisted by telecommunications
2 companies. *See, e.g.*, Am. Compl. ¶¶ 5-8, 70. The DNI again has demonstrated that disclosure
3 of whether the NSA has had an intelligence relationship with private companies would also cause
4 exceptional harm to national security by, among other things, revealing to foreign adversaries the
5 channels of communication that may or may not be secure. *See* Public DNI Decl. ¶ 17; Public
6 NSA Decl. ¶ 21.

7 In sum, the DNI's state secrets privilege assertion is amply supported and clearly
8 demonstrates there is a reasonable danger that disclosure of the privileged information would
9 cause exceptionally grave harm to national security. The privilege assertion should therefore be
10 upheld and the information described by the DNI and NSA Director should be excluded from
11 further proceedings in this case.

12 **C. The DNI and NSA Director Have Properly Raised Statutory Privileges to**
13 **Exclude Information Concerning Intelligence Sources and Methods From**
14 **This Case.**

15 In addition to the DNI's assertion of the state secrets privilege, both the DNI and the
16 Director of the NSA have asserted statutory privileges to protect the privileged information at
17 issue in this case. These statutory protections underscore that the exclusion of the privileged
18 information at issue is not only supported by the judgment of the Executive branch, but pursuant
19 to congressional authority as well. *Cf. Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579,
20 635 (1952) (Jackson, J., concurring) ("When the President acts pursuant to an express or implied
21 authorization of Congress, his authority is at its maximum, for it includes all that he possesses in

22 ¹¹(...continued)
23 of their communications. *See* Am. Compl. ¶¶ 2, 87, 110. Plaintiffs also allege in passing that the
24 NSA collects telephone "call data," *see id.* ¶ 58, but unlike the plaintiffs in the *Jewel* action do not
25 specifically raise a cause of action related to that allegation. *See id.* Count I (alleging plaintiffs were
26 subject to electronic surveillance under the FISA); Count II (alleging the contents of plaintiffs'
27 communications were intercepted in violation of the Wiretap Act); Count III (alleging unlawful
28 access to stored communications under 18 U.S.C. § 2701, but not alleged unlawful access to records
under 18 U.S.C. § 2703(c)); Count IV (alleging Fourth Amendment seizure of the content of
communications). To the extent plaintiffs' allegations implicate the alleged collection of telephone
call data, the DNI has also explained that confirmation or denial of whether the NSA has collected
communications records would cause exceptionally grave harm to national security. *See* Public DNI
Decl. ¶ 16.

1 his own right plus all that Congress can delegate.”). Section 6 of the National Security Agency
2 Act of 1959, Pub. L. No. 86-36, § 6, 73 Stat. 63, 64 (codified at 50 U.S.C. § 402 note), forecloses
3 “disclosure of the organization or any function of the National Security Agency, of any
4 information with respect to the activities thereof” Likewise, Section 102A(i)(1) of the
5 Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 10-458, 118 Stat. 3638
6 (Dec. 17, 2004) (codified at 50 U.S.C. § 403-1(i)(1)), requires the Director of National
7 Intelligence to protect intelligence sources and methods from unauthorized disclosure. The
8 information subject to these statutory privileges is coextensive with the assertion of the state
9 secrets privilege by the DNI and the NSA Director. *See* Public DNI Decl. ¶ 10; Public NSA
10 Decl. ¶ 23. Thus, all of the information subject to the DNI’s state secrets privilege assertion is
11 also subject to statutory protection and should be excluded from further litigation for this reason
12 as well.¹²

13 **III. SUMMARY JUDGMENT SHOULD BE ENTERED FOR THE GOVERNMENT**
14 **BECAUSE THE EVIDENCE NEEDED TO LITIGATE PLAINTIFFS’ STANDING**
15 **AND CLAIMS ON THE MERITS IS PROPERLY EXCLUDED BY THE STATE**
16 **SECRETS AND RELATED STATUTORY PRIVILEGES.**

17 Once a court has upheld a claim of the state secrets privilege, the evidence and
18 information identified in the privilege assertion is “completely removed from the case,” *Kasza*,
19 133 F.3d at 1166, and the court must undertake a separate inquiry to determine the consequences
20 of this exclusion on further proceedings. If the plaintiffs cannot establish their standing as a
21 factual matter without the excluded state secrets, then the privilege assertion (unless preempted)
22 would require dismissal. *See Al-Haramain*, 507 F.3d at 1204-05. Similarly, if the plaintiffs
23 cannot make out a *prima facie* case in support of their claims absent the excluded state secrets,

24 ¹² Courts have applied the NSA and DNI statutory privileges to protect information
25 specifically related to whether individuals have been subject to surveillance under the Terrorist
26 Surveillance Program. In *People for the American Way Found v. NSA (PFAW)*, 462 F. Supp. 2d 21
27 (D.D.C. 2006), the court applied Section 6 of the National Security Agency Act to bar disclosure
28 under FOIA of information related to the operation of the TSP, including whether the plaintiffs in
that case had been subject to TSP surveillance, and recognized as well that this information would
be protected by the DNI’s statutory privilege. *See id.* at 29, 31 & n.8. Likewise, in *Wilner v. NSA*,
No. 07 Civ. 3883, 2008 WL 2567765, at **4-5 (S.D. N.Y. June 25, 2008) (appeal pending), the court
applied Section 6 to bar disclosure of whether the plaintiffs had been subject to TSP surveillance.

1 the court should enter summary judgment for the United States because the evidence needed to
2 adjudicate the merits is unavailable. *See Kasza*, 133 F.3d at 1176 (affirming entry of summary
3 judgment for the United States on state secrets privilege grounds). Likewise, ““if the privilege
4 deprives the *defendant* of information that would otherwise give the defendant a valid defense to
5 the claim, then the court may [also] grant summary judgment to the defendant.”” *Kasza*, 133
6 F.3d at 1166 (quoting *Bareford v. General Dynamics Corp.*, 973 F.2d 1138, 1141 (5th Cir.
7 1992)) (emphasis in original); *see also Zuckerbraun v. General Dynamics Corp.*, 935 F.2d 544,
8 547 (2d Cir. 1991).¹³ As set forth below, the facts needed for plaintiffs to establish standing or
9 litigate the merits of all their claims against all defendants are subject to the DNI’s privilege
10 assertion and are unusable in this case.¹⁴

12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

¹³ Courts have also considered the related question of whether the “very subject matter” of a case is a state secret warranting dismissal as a threshold matter. *See Al-Haramain*, 507 F.3d at 1197-1201; *Kasza*, 133 F.3d at 1166 (citing *Reynolds*, 345 U.S. at 11 n.26). The Ninth Circuit has recognized that “a bright line does not always separate the subject matter of the lawsuit from the information necessary to establish a *prima facie* case,” and that “[i]n some cases, there may be no dividing line.” *Al-Haramain*, 507 F.3d at 1201; *see also Kasza*, 133 F.3d at 1170 (finding that the very subject matter of the case is a state secrets because “[n]ot only does the state secrets privilege bar [plaintiff] from establishing her *prima facie* case on any of her eleven claims, but any further proceeding in this matter would jeopardize national security”). At any rate, in some 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.” *Al-Haramain*, 507 F.3d at 1201. Plaintiffs in this case do not challenge the publicly-acknowledged (now defunct) TSP, but allege that other activities were authorized after 9/11 and are ongoing. Because litigation of plaintiffs’ claims would inherently risk or require the disclosure of privileged intelligence sources and methods, dismissal would be appropriate on the ground that the very subject matter of this case is a state secret. To be clear, however, the Government does not seek dismissal merely on this basis, but seeks summary judgment, as permitted by *Kasza*, on the ground that the Government’s privilege assertions exclude the very information necessary for plaintiffs to establish their standing or a *prima facie* case, as well as information relevant to any defense by the defendants.

¹⁴ The Government construes the Amended Complaint to allege official capacity claims only. This is because the Amended Complaint does not clearly identify whether particular defendants are being sued in their official and/or personal capacity, does not make specific allegations against any of the defendants in their personal capacity and does not state whether plaintiffs are seeking money damages against any of the defendants in their individual capacity. In any event, the Government’s instant motion seeks dismissal of all claim against all defendants, regardless of the capacity in which they may be sued, on the ground that the information necessary for plaintiffs to establish standing and litigate such claims is properly excluded by the Government’s privilege assertions.

1 **A. Plaintiffs Cannot Establish Their Standing Without the Disclosure of**
2 **Information Subject to the DNI's Privilege Assertion.**

3 The fundamental, threshold issue of plaintiffs' standing to bring this suit cannot be
4 adjudicated without risking or requiring the disclosure of state secrets, and this alone forecloses
5 the case from proceeding. Plaintiffs, of course, bear the burden of establishing their standing and
6 must, at an "irreducible constitutional minimum," demonstrate (1) an injury-in-fact, (2) a causal
7 connection between the injury and the conduct complained of, and (3) a likelihood that the injury
8 will be redressed by a favorable decision. *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 559-60
9 (1992). In meeting that burden, plaintiffs must demonstrate an actual or imminent—not
10 speculative or hypothetical—injury that is particularized as to them; they cannot rely on alleged
11 injuries to unnamed members of a purported class. *See, e.g., Warth v. Seldin*, 422 U.S. 490, 502
12 (1975); *see also Ellsberg*, 709 F.2d at 65. Moreover, to obtain prospective relief, plaintiffs must
13 show that they are currently subject to an alleged activity or otherwise "immediately in danger of
14 sustaining some direct injury" as the result of the challenged conduct. *City of Los Angeles v.*
15 *Lyons*, 461 U.S. 95, 102 (1983). Plaintiffs cannot rest on general allegations in their Amended
16 Complaint, but must set forth specific facts that establish their standing to obtain the relief
17 sought. *See Lewis v. Casey*, 518 U.S. 343, 358 (1996) (citing *Lujan*, 504 U.S. at 561).

18 Here, the DNI has properly asserted privilege over facts essential for plaintiffs to establish
19 their standing, and courts have consistently deferred to such determinations and recognized that
20 dismissal is necessary in these circumstances. For example, in a case related to this one, *Al-*
21 *Haramain*, the Ninth Circuit upheld the Government's state secrets privilege assertion at the
22 outset of litigation, before consideration of any particular discovery requests. Indeed, the *Al-*
23 *Haramain* Court considered the privilege assertion despite its conclusion that the case did not fall
24 into the narrow category of suits that cannot be litigated as a result of the *Totten* doctrine. *See*
25 *507 F.3d at 1201-05*. Rather, the Court held that the plaintiffs there—similar to these
26 plaintiffs—could not establish standing without disclosure of state secrets, and the action would
27 therefore have to be dismissed (unless preempted by the FISA). *See id.*

28 Likewise, in *Terkel v. AT&T Corp.*, 441 F. Supp. 2d 899 (N.D. Ill. 2006), the court
dismissed a claim implicated by plaintiffs' allegations here—whether a telecommunications

1 company assisted the Government in alleged intelligence activities—on the ground that the state
2 secrets privilege foreclosed plaintiffs from establishing their standing. *See* 441 F. Supp. 2d at
3 919-20. The Sixth Circuit has also rejected standing based on a “well founded belief”—as
4 opposed to actual evidence—that communications were being intercepted under the TSP. *See*
5 *Am. Civil Liberties Union v. NSA*, 493 F.3d 644, 656 (6th Cir. 2007) (where state secrets
6 privilege prevents discovery of evidence of standing, allegations of harm held to be speculative
7 and insufficient to establish standing); *see also id.* at 692 (Gibbons, J., concurring) (dismissal
8 required where state secrets privilege prevents plaintiffs from establishing whether they were
9 subject to the TSP); *Halkin II*, 690 F.2d at 998 (holding that plaintiffs’ inability to adduce proof
10 of actual acquisition of their communications rendered them incapable of making the showing
11 necessary to establish their standing to seek relief); *Ellsberg*, 709 F.2d at 51 (holding that
12 dismissal was warranted where a plaintiff could not, absent recourse to state secrets, establish
13 that he was actually subject to surveillance); *cf. Amnesty Int’l v. McConnell*, —F. Supp. 2d—,
14 2009 WL 2569138 (S.D.N.Y. 2009) (granting summary judgment to Government after finding
15 plaintiffs lacked standing to assert pre-enforcement facial challenge to the FISA Amendment
16 Acts of 2008 based on fear of surveillance); *PFAW*, 462 F. Supp. 2d at 28-32 (barring disclosure
17 under FOIA of information related to the TSP); *Wilner*, 2008 WL 2567765, at **4-8 (barring
18 disclosure under FOIA of whether plaintiffs had been subject to surveillance under the TSP).

19 Similarly, the evidence defendants would need to address or disprove plaintiffs’
20 allegations of standing is also covered by the state secrets privilege assertion—for example,
21 evidence that a particular person’s communications may not have been intercepted. *See Am.*
22 *Civil Liberties Union*, 493 at 692 (Gibbons, J., concurring) (noting that dismissal is required
23 where the privilege prevents the Government from presenting evidence to refute such an
24 allegation); *see also Kasza*, 133 F.3d at 1166 (noting that summary judgment is appropriate “‘if
25 the privilege deprives the *defendant* of information that would otherwise give the defendant a
26 valid defense to the claim’”) (quoting *Bareford*, 973 F.2d at 1141); *Halkin I*, 598 F.2d at 11
27 (rejecting contention that acquisition of plaintiff’s communication may be presumed from certain
28 facts because “such a presumption would be unfair to the individual defendants who would have

1 no way to rebut it”).

2 The Government’s privilege assertion also precludes plaintiffs from establishing standing
3 as to any statutory claim that may survive the Government’s motion to dismiss. For each cause
4 of action they raise, plaintiffs must establish, as a threshold matter, that they have been
5 “aggrieved”—that is, subject to the alleged action being challenged.¹⁵ However, because
6 plaintiffs cannot adduce proof that their communications have been collected by the Government,
7 the most basic element of every statutory cause of action—their standing as “aggrieved
8 persons”—cannot be established. It bears emphasis that plaintiffs’ allegation of a “dragnet” of
9 surveillance by the NSA—the alleged interception of communication content of millions of
10 domestic and international communications made by ordinary Americans, *see, e.g.*, Am. Compl.
11 ¶ 2—does not establish their standing. Even if that bare allegation were sufficient to avoid
12 dismissal on the pleadings,¹⁶ plaintiffs would be required to demonstrate that they personally
13 have been subject to the alleged communications dragnet, and the information relevant to doing
14 so is properly protected by the state secrets privilege. That is, plaintiffs cannot establish the
15 existence of their alleged content dragnet (previously denied by the Government, *see Hepting*,

16
17 ¹⁵ With respect to plaintiffs’ claim for damages under 50 U.S.C. § 1810, the term “aggrieved
18 person” under the FISA is “coextensive [with], but no broader than, those persons who have standing
19 to raise claims under the Fourth Amendment with respect to electronic surveillance,” H.R. REP. NO.
20 95-1283 at 66 (1978); *see Rakas v. Illinois*, 439 U.S. 128, 132 n.2 (1978) (noting that a party raising
21 a Fourth Amendment claim “must allege such a personal stake or interest in the outcome of the
22 controversy as to assure the concrete adverseness which Art. III requires”). Similarly, under the
23 Wiretap Act, 18 U.S. C. § 2510, civil actions may be brought only by a “person whose . . .
24 communication is intercepted, disclosed, or intentionally used.” 18 U.S.C. § 2520(a). The Stored
25 Communication Act likewise limits its civil remedies to “person[s] aggrieved” under the statute, *id.*
26 § 2707(a); *see id.* 2711(1) (adopting Section 2510(11) definition of “aggrieved person” as one “who
27 was a party to any intercepted . . . communication” or “a person against whom the interception was
28 directed”). Each of these provision 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 have Article III standing to proceed.

26 ¹⁶ The Court could find that plaintiffs’ allegations of injury are too speculative and
27 conjectural to satisfy Article III standing requirements at the pleading stage. Plaintiffs are merely
28 speculating that the alleged dragnet surveillance exists and encompasses their communications. As
set forth herein, plaintiffs’ standing could never be confirmed or denied as a factual matter in light
of the Government’s privilege assertion, and that forecloses further proceedings even if plaintiffs
have sufficiently alleged an injury.

1 439 F. Supp. 2d at 996), or, critically for the statutory cause of action, its application to them
2 personally, without risking or requiring disclosure of NSA intelligence sources and methods. For
3 this reason, plaintiffs cannot sustain their burden of showing that such a program exists, much
4 less satisfy their burden of establishing standing by showing that *their* communications were
5 collected under such an alleged program, and their action must be dismissed for failing to meet
6 the constitutional and statutory standing requirements.

7 Finally, to the extent implicated by their allegations, plaintiffs could not establish
8 standing as to whether their telephone “call data” was collected as part of (or apart from) the
9 alleged communications dragnet. As this Court noted in *Hepting*, “the government has neither
10 confirmed nor denied whether it monitors communication records and has never publicly
11 disclosed whether [such a program] actually exists,” *see* 439 F. Supp. 2d at 997, and the Court
12 further recognized, in barring discovery on this claim in *Hepting*, that:

13 Revealing that a communication records program exists might
14 encourage that terrorist to switch to less efficient but less
15 detectable forms of communication. And revealing that such a
 program does not exist might encourage a terrorist to use AT&T
 services when he would not have done so otherwise.

16 *Id.*; *accord*, *Terkel*, 441 F. Supp. 2d at 917. The Government’s privilege assertion as to this
17 allegation again demonstrates the exceptional harm to national security that would result from
18 any further proceedings on this allegation. For this reason, plaintiffs cannot sustain their burden
19 of showing that such a program exists, nor establish standing by showing that *their* telephone
20 records were collected under such an alleged program.

21 **B. The Disclosure of Privileged Information Would Also Be At Risk or**
22 **Required to Adjudicate Plaintiffs’ Claims on the Merits.**

23 Beyond the fact that plaintiffs cannot establish standing without resort to privileged
24 information, information subject to the Government’s state secrets and statutory privilege
25 assertions would be required to litigate plaintiffs’ claims on the merits. For example, plaintiffs’
26 claim that they were subject to a “dragnet” of content surveillance would require proof not only
27 of an alleged interception of their communications, but that any such interception met the highly
28 specific definition of “electronic surveillance” under the FISA, which includes, among other
things, that a communication be intercepted on a wire inside the United States. *See* 50 U.S.C.

1 § 1809; *id.* § 1801(f). This would require disclosure of specific facts concerning where and how
2 any communications were intercepted (if any)—information that would reveal precise
3 intelligence sources and methods through which content may, or may not, be captured by the
4 Government. Another element of plaintiffs’ FISA claim would require proof that the
5 Government intentionally disclosed or used information obtained under color of law by
6 electronic surveillance, knowing or having reason to know the information was obtained through
7 unauthorized electronic surveillance. *See* 50 U.S.C. § 1809. Thus, assuming the content of their
8 communications had been intercepted at all, plaintiffs still would have to show an intentional
9 disclosure or use of that information to support this aspect of their FISA claim—information that,
10 again, would either reveal the existence of foreign intelligence interest in plaintiffs or their
11 communicants or, conversely, the lack thereof. In either case, the result would be the disclosure
12 of information revealing the scope of NSA intelligence sources, methods and activities and the
13 attendant risk of exceptionally grave harm to national security, against which the state secrets
14 privilege guards.

15 Likewise, plaintiffs’ Wiretap Act claim would require proof that one of plaintiffs’ wire or
16 electronic communications, as defined in the Act, *see* 18 U.S.C. § 2510 (1), (12), had been
17 intercepted—information that would reveal particular intelligence methods were or were not used
18 to target plaintiffs’ communications. If such an interception had occurred, plaintiffs must then
19 show that the content of their communications, defined to mean the “substance, meaning or
20 purport” of the communication, *see* 18 U.S.C. § 2510(8), was knowingly disclosed and used in
21 violation of the Act, *see* 18 U.S.C. § 2511(1)(c), (d). Again, this they cannot do without the
22 disclosure of intelligence sources, methods and activities properly subject to the state secrets
23 privilege.

24 Similarly, plaintiffs’ claim under Stored Communications Act would require proof that
25 their “electronic communications” were intentionally accessed in electronic storage, *see* 18
26 U.S.C. § 2701, which again would require or risk disclosure of intelligence sources, methods and
27 activities regarding whether or not, or when and how, the content of plaintiffs’ wire or electronic
28 communications were obtained by the Government.

1 To the extent plaintiffs have raised a Fourth Amendment claim, litigation of that matter
2 would put at issue not only whether their individual communications were collected, but whether
3 there existed a reasonable basis for the particular search or seizure, whether exigent
4 circumstances warranted any action at issue, and what specific information was actually
5 obtained, viewed, used, or disclosed by the Government. Such Fourth Amendment claims
6 require fact-specific determinations, including whether a search was undertaken, under what
7 authority, whether it violated an expectation of privacy, and why the Government may have
8 acted. *See, e.g., O'Connor v. Ortega*, 480 U.S. 709, 718 (1987) (noting that “what is reasonable
9 depends on the context within which a search takes place”) (quoting *New Jersey v. T.L.O.*, 469
10 U.S. 325, 337 (1985)). Addressing or attempting to refute plaintiffs’ Fourth Amendment claim
11 would thus require the Government to disclose intelligence sources and methods, or the lack
12 thereof—the very information protected by the Government’s privilege assertions. *See, e.g.,*
13 *Kasza*, 133 F.3d at 1166.¹⁷

14 In addition, as to all of the foregoing claims, to the extent that plaintiffs allege the
15 participation of telecommunications carriers, they again would have to obtain confirmation or
16 denial as to whether any telecommunications company participated in the alleged activity, as well
17 as where, how, and to what extent they were involved, to determine if any such participation
18 implicated plaintiffs’ communications. The DNI has set forth a more than reasonable basis to
19 conclude that exceptionally grave harm to national security would result from the disclosure of
20 whether the NSA has worked with any telecommunications carrier in conjunction with the
21

22 ¹⁷ There may be no Fourth Amendment issue at all if the Government only obtained non-
23 content information. *See, e.g., Smith v. Maryland*, 442 U.S. 735, 742-46 (1979) (holding that
24 individuals have no legitimate expectation of privacy in the numbers they dial on the telephone and
25 pen register search of such information does not constitute a search for Fourth Amendment
26 purposes); *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2007) (“[E]-mail and Internet
27 users have no expectation of privacy in the to/from addresses of their messages or the IP addresses
28 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.”). In any
event, to the extent plaintiffs’ Amended Complaint places the alleged collection of telephone call
data at issue, litigation of any such claim would require confirmation or denial of that alleged activity
and, if it did exist, whether it applied in particular to plaintiffs’ records—again revealing information
protected by the Government’s privilege assertions.

1 alleged activities. Public DNI Decl. ¶¶ 14, 16-17. Indeed, this Court previously has observed
2 that it is not in a position to second-guess the DNI’s judgment regarding a terrorist’s risk
3 preferences for picking a communications carrier, and thus the need to invoke the state secrets
4 privilege—a judgment that might depend on an array of facts not before the Court.¹⁸ See
5 *Hepting*, 439 F. Supp. 2d at 990, 997.

6 To the extent plaintiffs’ claims allege the cooperation of telecommunications companies
7 in any supposed intelligence activities, see Am. Compl. ¶¶ 5-8, such assertions are also squarely
8 foreclosed by the *Totten* doctrine. The Supreme Court explicitly has stated that litigation risking
9 the disclosure of an espionage relationship is barred *per se*: “The possibility that a suit may
10 proceed and an espionage relationship may be revealed . . . is unacceptable: ‘Even a small chance
11 that some court will order disclosure of a source’s identity could well impair intelligence
12 gathering and cause sources to “close up like a clam.”’” *Tenet v. Doe*, 544 U.S. 1, 11 (2005)
13 (quoting *Sims*, 471 U.S. at 175); see *Totten*, 92 U.S. at 106-07; see also *Terkel*, 441 F. Supp. 2d
14 at 917 (upholding privilege assertion with respect to similar claim).¹⁹ Plaintiffs’ allegations, to
15 the extent they implicate any alleged relationship between the NSA and telecommunications
16

17 ¹⁸ The DNI is not alone in recognizing the exceptionally grave harm that might result from
18 disclosing an intelligence agencies cooperative relationships, if any. In enacting the FISA Act
19 Amendments Act of 2008, the Senate Select Committee on Intelligence (“SSCI”) found that the
20 “details of the President’s program are highly classified” and that, as with other intelligence matters,
21 the identities of persons or entities who provide assistance to the U.S. Government are protected as
22 vital sources and methods of intelligence.” See S. REP. 110-209 (2007) (Dkt. 469-2, Ex.1 at 10 in
23 MDL 06-cv-1791-VRW). Notably, the SSCI expressly stated that “[i]t would be inappropriate to
24 disclose the names of the electronic communication service providers from which assistance was
25 sought, the activities in which the Government was engaged or in which providers assisted, or the
26 details regarding any such assistance,” because “identities of persons or entities who provide
27 assistance to the intelligence community are properly protected as sources and methods of
28 intelligence.” *Id.*

25 ¹⁹ A panel of the Ninth Circuit construed the *Totten* bar narrowly in *Mohamed v. Jeppesen*
26 *Dataplan, Inc.*, 579 F.3d 943 (9th Cir. amended Aug. 31, 2009). On October 27, 2009, the Ninth
27 Circuit ordered *Jeppesen* to be reheard *en banc*. See *Mohamed v. Jeppesen Dataplan, Inc.*, No. 08-
28 15693 (9th Cir. Oct. 27, 2009) (Dkt. 7109126). Given that order, the panel’s *Jeppesen* decision is
not precedent to this or any other court of the Ninth Circuit. *Id.*; Ninth Cir. R. 35-3 advisory
committee’s note; Ninth Cir. Gen. Order 5.5(d).

1 companies, must be dismissed for this independent reason as well.

2 Adjudication of the merits would require disclosure of whether any of the alleged
3 activities, if they exist, are ongoing, or occurred only during certain periods, or were authorized
4 at some point by statute or court order. Disclosure of such information would be relevant not
5 only to the question whether any prospective relief is appropriate, but also whether plaintiffs may
6 seek damages for any past alleged violation. In either case, such disclosures again would reveal a
7 range of facts concerning whether, when, how, why, and under what authority the NSA may have
8 utilized certain intelligence sources and methods—information that is subject to the
9 Government’s privilege assertion and cannot be disclosed without risking exceptionally grave
10 harm to national security.

11 The law is clear that dismissal of an action based on an assertion of the state secrets
12 privilege is required where adjudication of the claims would risk disclosing information
13 protected by the privilege. This result is necessary when the Government’s privilege assertion
14 protects from disclosure facts concerning intelligence sources and methods that are central not
15 only to standing but to plaintiffs’ ability to establish a *prima facie* case, such as the threshold
16 questions here whether or not the NSA used alleged sources or methods to collect the content of
17 their communications or received assistance from telecommunications carriers. Thus, in *Kasza*
18 *v. Browner, supra*, the Ninth Circuit rejected an approach that would have litigation continue in
19 the face of a proper privilege assertion, without requiring the Government, for example, to wait
20 for plaintiffs’ discovery requests and assert the privilege for each one. The Court concluded that
21 the responsible official could not “reasonably be expected personally to explain why each item of
22 information arguably responsive to a discovery request affects the national interest.” *Kasza*, 133
23 F.3d at 1169. Rather, the court in *Kasza* affirmed summary judgment for the Government when
24 it was apparent that the information necessary for plaintiffs to establish their *prima facie* case or
25 for the Government to defend was properly protected by the state secrets privilege. *See also*
26 *Zuckerbraun*, 935 F.2d at 545 (“[T]he government properly invoked the state secrets privilege
27 and thereby prevented [the plaintiff from] establish[ing] a *prima facie* case.”); *id.* at 547
28 (“[D]ismissal [under such circumstances] is probably most appropriate under Rule 56 on the

1 ground that plaintiff, who bears the burden of proof, lacks sufficient evidence to carry that
2 burden.”); *Fitzgerald v. Penthouse Int’l Ltd.*, 776 F.2d 1236, 1241-42 (4th Cir. 1985) (“[I]n some
3 circumstances sensitive military secrets will be so central to the subject matter of the litigation
4 that any attempt to proceed will threaten disclosure of the privileged matters.”); *Farnsworth*
5 *Cannon, Inc. v. Grimes*, 635 F.2d 268, 281 (4th Cir. 1980) (en banc) (“It is evident that any
6 attempt on the part of the plaintiff to establish a prima facie case would so threaten disclosure of
7 state secrets that the overriding interest of the United States and the preservation of its state
8 secrets precludes any further attempt to pursue this litigation.”).

9 As in *Kasza*, it is apparent in this case that plaintiffs cannot establish a *prima facie* case
10 without risking or requiring the disclosure of information protected by the state secrets privilege
11 assertion. In response to the Government’s prior motion in this case, plaintiffs submitted an
12 affidavit pursuant to Rule 56(f) of the Federal Rules of Civil Procedure (*see* Declaration of Ilann
13 M. Maazel pursuant to Rule 56(f), Dkt. 12) (“Maazel Decl.”), which establishes that the evidence
14 sought in discovery by plaintiffs falls squarely within the Government’s privilege assertion.²⁰
15 Plaintiffs seek “discovery on telecommunications carriers . . . seeking information on the
16 interception and disclosure of plaintiffs’ communications to the Government.” Maazel Decl. ¶ 5;
17 *see also id.* ¶ 9 (seeking “the facts of the telecommunications carriers’ interception of plaintiffs’
18 communications for the Government”); ¶ 10 (seeking “the facts of telecommunications carriers’
19 disclosure of plaintiffs’ communications to the Government”); ¶ 14 (seeking to take depositions
20 of telecommunication company executives regarding alleged interception). Other discovery
21 sought by plaintiffs likewise is plainly intended to uncover information concerning the scope and
22 other details of the alleged intelligence activities. *See* Maazel Decl. ¶¶ 7, 8 (seeking to propound
23

24
25 ²⁰ The evidence sought by plaintiffs here is substantially the same as sought by plaintiffs in
26 the *Jewel* action (*see* Declaration of Cindy Cohn Pursuant to Fed. R. Civ. P. 56(f), Dkt. 30 in No.
27 08-cv-4373-VRW), and also incorporates discovery requests propounded by plaintiffs in the
28 telecommunications carrier litigation (*see* Declaration of Candace J. Morey, Dkt. 316 in MDL 06-cv-
1791-VRW). The similarity of proposed discovery requests among these various actions is not
surprising because, as noted throughout this submission, the different plaintiffs’ ability to
demonstrate their standing or *prima facie* cases depends on the same core allegations—all of which
squarely implicate information protected by the state secrets privilege.

1 discovery to determine the scope and existence of the alleged “content monitoring program”);²¹
2 *id.* ¶ 11 (seeking “information on [telecommunications carriers’] network architecture and the
3 manner in which they intercept plaintiffs’ communications”); *id.* ¶ 13 (seeking “disclos[ure]” of
4 “aspects of the spying program” from “government employees”).

5 It should be readily apparent, therefore, that plaintiffs, in an attempt to prove their case,
6 seek discovery of the very sources and methods of intelligence collection that the Government’s
7 privilege assertion seeks to protect, including with respect to the alleged role of
8 telecommunications companies in alleged intelligence activities. *See* Public DNI Decl. ¶¶ 14,
9 16-17; Public NSA Decl. ¶ 21. There is nothing hypothetical about the role that privileged
10 evidence will play in this litigation—plaintiffs have provided a detailed roadmap of that
11 evidence—and, thus, there is nothing that should foreclose a determination now that the facts
12 central to the resolution of this case have been properly protected by the state secrets privilege in
13 order to prevent harm to national security. It should also be clear that defending against the
14 distinct factual allegation at issue here is impossible without compromising information subject
15 to the privilege assertions. In these circumstances, consistent with both *Al-Haramain*, *see supra*
16 Part III.A, and *Kasza*, the case cannot proceed.²²

17 Indeed, this case is in essentially the same posture as the *Frost* litigation, in which the
18 *Kasza* Circuit ultimately upheld summary judgment at the same stage of the proceedings. *Kasza*,
19 133 F.3d at 1159. According to published decisions in that case, the *Frost* plaintiffs first
20 propounded an interrogatory to the Government seeking the identity of a classified government
21 facility, which was met by the Government’s assertion of the state secrets privilege. *Frost v.*

22
23 ²¹ Plaintiffs also seek to obtain discovery from “confidential sources” quoted in news reports
24 describing the alleged surveillance in order “to overcome any possible hearsay objections.” Maazel
25 Decl. ¶ 12.

26 ²² Nor should the Court allow any attempt by plaintiffs to present non-privileged evidence
27 before determining that summary judgment is appropriate. There simply are no non-privileged facts
28 at issue here. Plaintiffs cannot make out a *prima facie* case based solely on their speculation from
public information. And it is apparent from the Maazel Declaration that plaintiffs ultimately cannot
demonstrate their standing or entitlement to relief without establishing facts directly at issue in the
privilege assertion itself.

1 *Perry (Frost I)*, 161 F.R.D. 434 (D. Nev. 1995). The district court held in May 1995 that the
2 Government could not be compelled to answer this interrogatory in the face of this broad, proper
3 invocation of the privilege. *Id.* at 436-37. Then, one month later, the Government moved for
4 summary judgment, which was briefed by the parties. *Frost v. Perry (Frost II)*, 919 F. Supp.
5 1459, 1462 (D. Nev. 1996). In response, the plaintiffs submitted an affidavit from counsel “to
6 counter the Defendants’ assertions that they cannot establish a *prima facie* case,” *id.* at 1467,
7 which cited photographs and two under seal declarations offered by the plaintiffs, *see id.*
8 Plaintiffs also brought various motions to compel discovery they sought. *See id.* at 1465-66.
9 These efforts to defeat the Government’s privilege assertion were rejected by the district court;
10 rather, the state secrets privilege was upheld and summary judgment entered for the Government
11 before any discovery was produced.²³

12 Thus, *Frost* and *Kasza* require disposition of the Government’s motion for summary
13 judgment where it is apparent that privileged evidence is essential to litigate the case (indeed, for
14 both sides) and that the evidence has been properly protected by the privilege assertion. Those
15 are the circumstances now before this Court, and summary judgment is likewise appropriate here.

16 **IV. LITIGATION OF PLAINTIFFS’ CLAIMS CANNOT PROCEED UNDER THE** 17 **FISA**

18 Finally, as noted above, the Government reserves its position that the state secrets
19 privilege is not preempted by Section 1806(f) of the FISA. We recognize the Court has
20 addressed this issue in the *Al-Haramain* action and, thus, the Government will not brief the
21 matter again at length here, but incorporates by reference its prior detailed discussion of the
22 issue. (*See* Memorandum of Points and Authorities in Support of Defendants’ Second Motion to
23 Dismiss or for Summary Judgment, Dkt. 17 at 12-24 in No. 07-cv-109-VRW; *see also*
24 Defendants’ Reply in Support of Defendants’ Second Motion to Dismiss or for Summary
25 Judgment, Dkt. 29 at 8-24 in No. 07-cv-109-VRW; Government Defendants’ Response to

26 ²³ Plaintiffs here, like the plaintiffs in the *Jewel* action, have relied on the panel opinion in
27 *Mohamed v. Jeppesen Dataplan, Inc.*, 579 F.3d 943 (9th Cir. amended Aug. 31, 2009), in asserting
28 that dismissal or summary judgment is not appropriate at this juncture. (*See, e.g.*, Dkt. 25 at 1). In
light of the Ninth Circuit’s decision to rehear that case *en banc*, however, *Jeppesen* is not precedent
in this or any other district court. *See supra* n.19.

1 Plaintiffs' Supplemental Brief, Dkt. 46 in No. 08-cv-4373-VRW (addressing claim of FISA
2 preemption of non-FISA claims)). In sum, we simply reiterate our position that the state secrets
3 privilege, which is rooted in the constitutional authority of the President as well as the common
4 law, cannot be preempted absent an unmistakably clear directive by Congress that it intended to
5 do so. Nothing in the text or legislative history of the FISA says anything about preempting the
6 state secrets privilege—let alone reflects a clear and unambiguous intention to do so.²⁴

7 CONCLUSION

8 For the foregoing reasons, the Court should dismiss plaintiffs' statutory claims for lack of
9 jurisdiction, uphold the Government's privilege assertions, and enter summary judgment for the
10 Government Defendants as to all defendants and all claims.

11
12 Date: October 30, 2009

Respectfully Submitted,

13 BETH S. BRINKMANN
14 Deputy Assistant Attorney General

15 DOUGLAS N. LETTER
16 Terrorism Litigation Counsel

17 JOSEPH H. HUNT
18 Director, Federal Programs Branch

19 VINCENT M. GARVEY
20 Deputy Branch Director

21
22
23
24
25
26
27 ²⁴ As in other cases in which the FISA preemption issue has arisen, the Court should not take
28 any action that could risk or require disclosure of the privileged information at issue, and thus negate
or moot the Government's privilege assertion through the use of Section 1806(f) procedures prior
to an opportunity for appellate review.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

s/ Anthony J. Coppolino
ANTHONY J. COPPOLINO
Special Litigation Counsel

s/ Marcia Berman
MARCIA BERMAN
Senior Trial Counsel

s/ Paul E. Ahern
PAUL E. AHERN
Trial Attorney

U.S. Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Avenue, NW, Rm. 6102
Washington, D.C. 20001
Phone: (202) 514-4782
Fax: (202) 616-8460

Attorneys for the Government Defendants