Kitagawa, Jr et al v. Apple, Inc. Doc. 29

ELECTRONIC FRONTIER FOUNDATION
CINDY COHN (SBN 145997)
cindy@eff.org
LEE TIEN (SBN 148216)
KURT OPSAHL (SBN 191303)
KEVIN S. BANKSTON (SBN 217026)
JAMES S. TYRE (SBN 083117)
454 Shotwell Street
San Francisco, California 94110
Telephone: (415) 436-9333; Facsimile: (415) 436-9993

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

LAW OFFICE OF RICHARD R. WIEBE
RICHARD R. WIEBE (SBN 121156)
wiebe@pacbell.net
425 California Street, Suite 2025
San Francisco, California 94104
Telephone: (415) 433-3200; Facsimile: (415) 433-6382

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

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

CAROLYN JEWEL, TASH HEPTING, GREGORY HICKS, ERIK KNUTZEN and JOICE WALTON, on behalf of themselves and all other similarly situated, Plaintiffs, v. NATIONAL SECURITY AGENCY, et al., Defendants.	Case No. C-08-4373-VRW CLASS ACTION **PLAINTIFFS' OPPOSITION TO GOVERNMENT DEFENDANTS' MOTION TO DISMISS AND FOR SUMMARY JUDGMENT** Date: July 15, 2009 Time: 10:30 a.m. Dept: 6, 17th Floor Judge: Vaughn R. Walker Date Comp. Filed: September 18, 2008

Dockets.Justia.com

TABLE OF CONTENTS

Page

INTRODUCTION 1

ARGUMENT 1

I. Sovereign immunity does not bar Plaintiffs' claims. 1

A. Congress waived sovereign immunity for Plaintiffs' damages claims. 1

1. Congress waived sovereign immunity for Plaintiffs' damages claims under the Wiretap Act and ECPA. 1

2. Congress waived sovereign immunity for Plaintiffs' damages claims under FISA. 4

B. Sovereign immunity does not bar Plaintiffs' equitable claims. 6

1. Plaintiffs' "*ultra vires*" claims alleging the Government Officer Defendants lack authority to conduct dragnet surveillance are not claims against the United States and thus cannot be barred by sovereign immunity. 6

2. Congress waived sovereign immunity for Plaintiffs' equitable relief claims, including Plaintiffs' APA claim. 12

II. For purposes of Plaintiffs' claims, FISA preempts the common-law state secrets privilege. 14

A. Where section 1806(f) applies, it preempts the common-law state secrets privilege. 15

B. FISA's section 1806(f) procedure applies to the evidence supporting all of Plaintiffs' claims. 16

III. Even if the state secrets privilege were not preempted, this case could not be dismissed based on the privilege. 18

A. The narrow "very subject matter" litigation bar is limited to secret agreements between a plaintiff and the executive, and does not apply here. 18

B. Defendants cannot dismiss this suit based on their speculative contention that future state secrets assertions will prevent presentation of evidence needed for Plaintiffs' prima facie case or Defendants' defenses. 19

CONCLUSION 24

TABLE OF AUTHORITIES

Page(s)

FEDERAL CASES

Adams v. City of Battle Creek
250 F.3d 980 (6th Cir. 2001) 5

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

Aminoil U.S.A., Inc. v. California State Water Resources Control Board
674 F.2d 1227 (9th Cir. 1982) 11

Assiniboine & Sioux Tribes v. Bd. of Oil & Gas
792 F.2d 782 (9th Cir. 1986) 12

Block v. N.D.
461 U.S. 273 (1983) 10, 13

Califano v. Sanders
430 U.S. 99 (1977) 12

Central Reserve Life Insurance Co. v. Struve
852 F.2d 1158 (9th Cir. 1988) 11

Chamber of Commerce v. Reich
74 F.3d 1322 (D.C. Cir. 1996) 8

Conner v. Tate
130 F. Supp. 2d 1370 (N.D. Ga. 2001) 5

Custis v. United States
511 U.S. 485 (1994) 2

Dorris v. Absher
959 F. Supp. 813 (M.D. Tenn. 1997) 5

Dugan v. Rank
372 U.S. 609 (1963) 11

Duncan v. Walker
533 U.S. 167 (2001) 3

Gilbert v. DaGrossa
756 F.2d 1455 (9th Cir. 1985) 5

Harmon v. Brucker
355 U.S. 579 (1958) 8

Hepting v. AT&T Corp.
439 F. Supp. 2d ..... *passim*

In re National Sec. Agency Telecomm. Records Litig.
564 F. Supp. 2d 1109 (N.D. Cal. 2008) ..... *passim*

Kasza v. Browner
133 F.3d 1159 (9th Cir. 1998) 15

Lane v. Pena
518 U.S. 187 (1996) 2

TABLE OF AUTHORITIES
(cont'd)

Page(s)

Larson v. Domestic & Foreign Commerce Corp.
337 U.S. 682 (1949) 7, 8, 9, 11

Mohamed v. Jeppesen Dataplan, Inc.
563 F. 3d 992 (9th Cir. 2009) ..... *passim*

Multi Denominational Ministry of Cannabis & Rastafari, Inc. v. Gonzales
474 F. Supp. 2d 1133 (N.D. Cal. 2007) 2, 5

North Side Lumber Co. v. Block
753 F.2d 1482 (9th Cir. 1985) 14

Organizacion JD Ltda. v. U.S. Dep't of Justice
18 F.3d 91 (2d Cir. 1994) 5

Palomar Pomerado Health System v. Belshe
180 F.3d 1104 (9th Cir. 1999) 12

PBA Local No. 38 v. Woodbridge Police Dep't
832 F. Supp. 808 (D. N.J. 1993) 5

Pennhurst State School & Hospital v. Halderman
465 U.S. 89 (1984) 11

Philadelphia Co. v. Stimson
223 U.S. 605 (1912) 8

Presbyterian Church (U.S.A.) v. U. S.
870 F.2d 518 (9th Cir. 1989) 12

Ratzlaf v. U. S.
510 U.S. 135 (1994) 3

Rochon v. Gonzales
438 F.3d 1211 (D.C. Cir. 2006) 5

S.E.C. v. Nacchio
__ F. Supp. 2d __, 2009 WL 690306 (D. Colo. Mar. 13 2009) 16

Salazar v. Heckler
787 F.2d 527 (10th Cir. 1986) 5

Totten v. United States,
92 U.S. 105 (1875) 19

Trudeau v. FTC
456 F.3d 178 (D.C. Cir. 2006) 12

United States v. King
395 U.S. 1 (1969) 14

United States v. Novak
476 F.3d 1041 (9th Cir. 2007) 6

Williams v. City of Tulsa
393 F. Supp. 2d 1124 (N.D. Okla. 2005) 6

Williams v. Fanning
332 U.S. 490 (1947) 11

TABLE OF AUTHORITIES
(cont'd)

Page(s)

FEDERAL STATUTES

5 U.S.C. § 702 ..... 12, 13

18 U.S.C.§ 2510 10

18 U.S.C. § 2511 ..... 6, 9, 14

18 U.S.C. § 2520 ..... *passim*

18 U.S.C. § 2707 ..... 2, 3, 5, 10, 13

18 U.S.C. § 2711 10

18 U.S.C. § 2712 ..... *passim*

28 U.S.C. § 1331 12

50 U.S.C. § 1801 ..... 4, 5

50 U.S.C. § 1806 ..... *passim*

50 U.S.C. § 1810 ..... *passim*

50 U.S.C. § 1812 ..... 9, 14

USA PATRIOT Act of 2001, Pub L. No. 107-56, 115 Stat. 272 ("PATRIOT") 3, 6

FEDERAL RULES

Fed. R. Civ. P. 25 7

Fed. R. Civ. P. 56 ..... 17, 23

CONSTITUTIONAL PROVISIONS

U.S. Const. amend. XI 11

OTHER AUTHORITIES

H.R. Conf. Rep. No. 95-1720 (1978), *reprinted in* 1978 U.S.C.C.A.N. 4048 17

U.S. Department of Justice, Searching & Seizing Computers and Obtaining Elect. Evidence in Crim. Investigations http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.pdf 4

INTRODUCTION

This case arises out of systemic, warrantless Government surveillance of the communications and communications records of millions of ordinary Americans, in violation of longstanding law and the Constitution. The Government Defendants Sued in their Official Capacity ("Defendants") here seek to bar judicial review of this evidence, effectively excluding the judicial branch from enforcing the privacy protections that the law and the Constitution provide to all Americans.

Defendants' Motion to Dismiss is almost wholly a rehash of sovereign immunity and state secrets arguments that this Court and the Ninth Circuit have soundly rejected; what little is new is equally meritless. The motion should be denied.

ARGUMENT

I. Sovereign immunity does not bar Plaintiffs' claims.

Defendants first argue that sovereign immunity shields them against Plaintiffs' claims for both damages and equitable relief. Neither argument succeeds.

A. Congress waived sovereign immunity for Plaintiffs' damages claims.

Congress has expressly waived sovereign immunity for all of Plaintiffs' damages claims under the Wiretap Act, the Electronic Communications Privacy Act (ECPA), and the Foreign Intelligence Surveillance Act (FISA). First, Congress waived sovereign immunity against Plaintiffs' counts IX, XII, and XV for violations of the Wiretap Act and ECPA according to the plain language of 18 U.S.C. § 2712(a), which authorizes suits against the United States for any willful violation of those statutes. Second, as this Court has ruled, in 50 U.S.C. § 1810 Congress waived sovereign immunity against claims such as count VI for unlawful electronic surveillance in violation of FISA. *In re Nat'l Sec. Agency Telecomm. Records Litig.*, 564 F. Supp. 2d 1109, 1124-25 (N.D. Cal. 2008) ("*Al-Haramain*").

1. Congress waived sovereign immunity for Plaintiffs' damages claims under the Wiretap Act and ECPA.

The plain language of 18 U.S.C. § 2712 expressly waives sovereign immunity and authorizes damages suits against the United States for "any willful violation" of any provision of

the Wiretap Act or ECPA. 18 U.S.C. § 2712(a). The statute provides:

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

18 U.S.C. § 2712(a) (line breaks added).

Ignoring this plain language, Defendants make the extraordinary claim that section 2712's waiver of sovereign immunity does not actually reach surveillance in violation of these laws. Instead, Defendants argue that the waiver is limited to violations of a few specific Wiretap Act and ECPA provisions that regulate the government's *disclosure* of information obtained pursuant to those statutes, *i.e.*, 18 U.S.C. §§ 2520(g) and 2707(g). *See* Gov't Br. at 5. However, as this Court has held, it is "[t]he plain language of the statute[] which the court must use as its primary compass." *Al-Haramain*, 564 F. Supp. 2d at 1134 (internal citation omitted). In this case, the compass's direction is unmistakable.

Section 2712's plain and unambiguous statement that the United States is subject to suit for any willful violation of any provision of ECPA or the Wiretap Act satisfies the rule that waivers of federal sovereign immunity "must be unequivocally expressed in statutory text." *Lane v. Pena*, 518 U.S. 187, 192 (1996); *see also Multi Denominational Ministry of Cannabis & Rastafari, Inc. v. Gonzales*, 474 F. Supp. 2d 1133, 1140 (N.D. Cal. 2007) (lawsuits for damages against federal employees in their official capacities "cannot be maintained unless Congress has explicitly waived the sovereign immunity of the United States."). If Congress had wished to limit section 2712's waiver to particular provisions of the Wiretap Act and ECPA, "it knew how to do so." *Custis v. United States*, 511 U.S. 485, 492 (1994). Indeed, Congress placed a specific limit on FISA causes of action in the very same sentence, waiving sovereign immunity only as to particular provisions of FISA not already subject to FISA's own waiver provisions. *See* 18 U.S.C. § 2712(a). No such limit, however, was placed on Wiretap Act or ECPA causes of action.

This plain language reading of 18 U.S.C. § 2712(a) is consistent with other provisions of

section 2712, provisions that Defendants' argument would render superfluous. A "cardinal principle of statutory construction" is that courts must "give effect, if possible, to every clause and word of a statute." *Duncan v. Walker*, 533 U.S. 167, 174 (2001) (internal quotations omitted). For instance, section 2712(b)(4) provides that actions brought under section 2712 must use the procedures set forth in 50 U.S.C. § 1806(f), which "shall be the exclusive means by which materials governed by th[at] section[] may be reviewed." The referenced section, 1806(f), then specifies that judicial review shall be "as may be necessary to determine *whether the surveillance of the aggrieved person was lawfully authorized and conducted*." 50 U.S.C. § 1806(f) (emphasis added). Congress thus anticipated and provided specific procedures for judicial consideration of the legality of surveillance in section 2712 cases against the United States. Section 2712(b)(4) would be rendered nugatory by Defendants' reading that the United States cannot be sued for any unlawful surveillance, but only for unlawful disclosures of surveillance-derived information. *See* Gov't Br. at 4-5.

Defendants willfully misread the statute when they counter that a plain language reading of 18 U.S.C. § 2712's sovereign immunity waiver would "emasculate" section 223 of the USA PATRIOT Act's other amendments to the Wiretap Act and ECPA. Gov't Br. at 4; USA PATRIOT Act of 2001, Pub L. No. 107-56, 115 Stat. 272 ("PATRIOT") at § 223(a)(1), (b)(1) (inserting the words "other than the United States" into the list of potential defendants in actions under 18 U.S.C. §§ 2520, 2707). Congress's purpose was not to eliminate all causes of action against the government for surveillance in violation of those statutes, but instead to *replace* the pre-existing causes of action under sections 2520 and 2707 with a new cause of action under section 2712 that provides new procedures and requirements specific to suits against the United States.

Defendants' resort to legislative history is both unnecessary and improper, because the plain language of section 2712 is clear. *See* Gov't Br. at 6; *Ratzlaf v. U. S.*, 510 U.S. 135, 147-48 (1994) (explaining that "we do not resort to legislative history to cloud a statutory text that is already clear"). Nonetheless, none of the history cited by Defendants supports their argument that Congress intended section 2712 to waive sovereign immunity *only* against claims for

unauthorized disclosures. Rather, that history merely confirms that a waiver for disclosure claims was *one* of that section's purposes. *See* Exhibits 3-5 to Gov't Br. (not indicating that disclosure concerns were section's only purpose).

In fact, when discussing liability for willful violations of ECPA, the Justice Department's own surveillance manual warns government agents that they may be sued for unauthorized disclosures under section 2712 *in addition* to being sued for illegal surveillance:

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

U.S. Dep't of Justice, Searching & Seizing Computers & Obtaining Elec. Evid. in Crim. Investigations, Section 2, at 109-110, available at http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.pdf (emphasis added).

2. Congress waived sovereign immunity for Plaintiffs' damages claims under FISA.

As this Court ruled in *Al-Haramain*, Congress waived sovereign immunity for FISA damages claims under 50 U.S.C. § 1810. *See* 564 F. Supp. 2d at 1124-25. Congress waived sovereign immunity in two ways. First, as this Court held, Congress waived immunity by expressly making federal officers acting in their official capacities subject to suit for damages. *See id.* Second, Congress also waived immunity by expressly making "any . . . entity," including the United States, subject to suit. *See* 50 U.S.C. § 1801(m) (defining "Person[s]" amenable to suit to include "any . . . entity").

FISA's provision for civil damages provides for relief against "any person" who conducts unlawful electronic surveillance, 50 U.S.C. § 1810, and as defined in FISA, a "person" includes "any officer or employee of the Federal Government." 50 U.S.C. § 1801(m). *Al-Haramain* explains:

> FISA directs its prohibitions to "Federal officers and employees" . . . and it is only such officers and employees acting in their official capacities that would engage in surveillance of the type contemplated by FISA. The remedial provision of FISA in section 1810 would afford scant, if any, relief if it did not lie against such

> "Federal officers and employees" carrying out their official functions. Implicit in the remedy that section 1810 provides is a waiver of sovereign immunity.

564 F. Supp. 2d at 1125 (internal citations omitted). That *Al-Haramain* holding flows directly from the rule, previously recognized by this Court, that an action seeking damages against federal officers and employees in their official capacities "is considered a suit against the United States." *Multi Denominational Ministry*, 474 F. Supp. 2d at 1140; *accord, Gilbert v. DaGrossa*, 756 F.2d 1455, 1458 (9th Cir. 1985). By prescribing civil damages liability for federal officers or employees—and hence the United States—through its definition of "person," FISA waives federal sovereign immunity despite the absence of an express specification of "the United States." *Cf. Salazar v. Heckler*, 787 F.2d 527, 528-529 (10th Cir. 1986) (Title VII of Civil Rights Act of 1964, which authorizes civil actions for employment discrimination by specifying "the head" of an offending federal entity as defendant, waives sovereign immunity despite failure to specify "the United States"); *accord, Rochon v. Gonzales*, 438 F.3d 1211, 1215-16 (D.C. Cir. 2006).

FISA also waives sovereign immunity by its inclusion of "any ... entity" in its definition of "person[s]" amenable to suit under 50 U.S.C. § 1810. *See* 50 U.S.C. § 1801(m) (defining "person"). Prior to 2001, FISA, the Wiretap Act, and ECPA each imposed liability on "any . . . entity," including the United States. *See Organizacion JD Ltda. v. U.S. Dep't of Justice*, 18 F.3d 91, 94-95 (2d Cir. 1994) (*per curiam*) (finding waiver of sovereign immunity against ECPA claims under 18 U.S.C. § 2707 based on statute's applicability to any "entity").[1] Congress preserved this understanding of "entity" in 2001, when it left FISA's provision unchanged while amending the Wiretap Act and ECPA civil causes of action by inserting "other than the United States" at the end of the list of potential defendants in those statutes, in order to exclude the United States from the entities liable under those two statutes. *See* PATRIOT § 223(a)(1) and

[1] *See also Adams v. City of Battle Creek*, 250 F.3d 980, 985-86 (6th Cir. 2001) ("entity" included governmental entities such that municipal government could be sued for Wiretap Act violations under 18 U.S.C. § 2520); *PBA Local No. 38 v. Woodbridge Police Dep't*, 832 F. Supp. 808, 823 (D. N.J. 1993) (same); *Dorris v. Absher*, 959 F. Supp. 813, 819-21 (M.D. Tenn. 1997) (same), *affirmed in part and reversed in part on other grounds*, 179 F.3d 420 (6th Cir. 1999); and *Conner v. Tate*, 130 F. Supp. 2d 1370, 1373-76 (N.D. Ga. 2001) (same under both ECPA and Wiretap Act).

(b)(1) (amending 18 U.S.C. §§ 2520, 2707). If the term "entity" did not already include the United States, those amendments would have been unnecessary and their language superfluous. *See Williams v. City of Tulsa*, 393 F. Supp. 2d 1124, 1132-33 (N.D. Okla. 2005) ("Congress' subsequent amendment in 2001 to exclude the United States from entities that could be liable [under the Wiretap Act] evidences a Congressional understanding that the 1986 amendment [adding 'entity' to the list of potential defendants in 18 U.S.C. § 2520] created governmental liability.").

Like the Wiretap Act and ECPA, FISA comprehensively regulates government surveillance of communications, and together with those statutes provides the "exclusive means" by which the government may conduct such surveillance. *See* 18 U.S.C. § 2511(2)(f). Therefore, this Court can and should read "entity" in FISA to include the United States, just as that same term was construed in the Wiretap Act and ECPA prior to PATRIOT. *See United States v. Novak*, 476 F.3d 1041, 1051 (9th Cir. 2007) (explaining courts should "interpret similar language in different statutes in a like manner when the two statutes address a similar subject matter"). If Congress had intended to create sovereign immunity against FISA damages suits under 50 U.S.C. § 1810 and to exclude the United States from the entities that are liable under that section, it would have had to insert "other than the United States" into the statute, as Congress did with the specific provisions of the Wiretap Act and ECPA that it amended in PATRIOT. It did not.

B. Sovereign immunity does not bar Plaintiffs' equitable claims.

1. Plaintiffs' "*ultra vires*" claims alleging the Government Officer Defendants lack authority to conduct dragnet surveillance are not claims against the United States and thus cannot be barred by sovereign immunity.

The sovereign immunity analysis for equitable relief claims against government officers is fundamentally different from the sovereign immunity analysis for damages claims. Here, Counts V, VII, X, and XIII seek equitable relief against Government Officer Defendants Alexander, Holder, and Blair on the grounds that they lack statutory authority for the dragnet surveillance they are conducting and that they are exceeding statutory limitations on their

authority.[2] Defendants' argument that sovereign immunity bars these claims ignores the fact that these "*ultra vires*" claims against government officers are not claims against the United States to which sovereign immunity attaches.[3]

An equitable relief claim to restrain a federal officer from exceeding the powers he or she has been granted by statute—an *ultra vires* claim—is not a claim against the United States, and for that reason it is not barred by sovereign immunity. The dividing line, as the Supreme Court explained in *Larson v. Domestic & Foreign Commerce Corp.*, 337 U.S. 682 (1949), is whether the claim alleges acts by the officer that, even if wrongful, are within the scope of the authority 337 U.S. at 690. Congress has granted or instead alleges acts by the officer beyond the limits of his or her authority. Only "if the actions of an officer do *not* conflict with the terms of his valid statutory authority, . . . are [they] the actions of the sovereign" and subject to sovereign immunity. *Id.* at 695 (emphasis added). Otherwise, "the conduct against which specific relief is sought is beyond the officer's powers and is, therefore, not the conduct of the sovereign," and sovereign immunity does not apply. *Id.*

As *Larson* explains:

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

---

[2] The automatic substitution provisions of Federal Rule of Civil Procedure 25(d)(1) for official-capacity claims substitute Defendants Holder and Blair for Defendants Mukasey and McConnell with respect to Plaintiffs' *ultra vires* claims brought under *Larson v. Domestic & Foreign Commerce Corp.*, 337 U.S. 682 (1949). Fed. R. Civ. Pro. 25(1) & 1961 amendment advisory comm. note (citing *Larson*; explaining that "[t]he expression 'in his official capacity' [in Rule 25(d)] is to be interpreted in its context as a simple procedural rule for substitution; care should be taken not to distort its meaning by mistaken analogies to the doctrine of sovereign immunity," and that Rule 25(d)'s official-capacity substitution "also appl[ies] to actions to prevent officers from acting in excess of their authority"). In Counts V, VII, X, and XIII, Plaintiffs seek equitable relief to confine the actions of Government Officer Defendants Alexander, Holder, and Blair within the statutory limits of their offices. As Rule 25(d) recognizes and as the text *infra* explains, these *Larson ultra vires* claims for equitable relief are official-capacity claims to which sovereign immunity does not attach.

[3] Defendants do not contest that Counts I, III, and XVII properly state claims for equitable relief against them for constitutional violations.

Id. at 689-690. Because actions beyond the limits set by Congress are not those of the sovereign, enjoining the officer from transgressing those limits does not enjoin any act of the sovereign and does not interfere with the authority or impose upon the discretion of the sovereign. Indeed, it is the sovereign that has imposed the statutory limits upon the officer that the officer is transgressing.

Thus, "under *Larson* . . ., if the federal officer, against whom injunctive relief is sought, allegedly acted in excess of his legal authority, sovereign immunity does not bar a suit . . . [T]here is no sovereign immunity to waive—it never attached in the first place." *Chamber of Commerce v. Reich*, 74 F.3d 1322, 1329 (D.C. Cir. 1996); *accord*, *Harmon v. Brucker*, 355 U.S. 579, 581-82 (1958) (explaining "judicial relief is available to one who has been injured by an act of a government official which is in excess of his express or implied powers"); *Philadelphia Co. v. Stimson*, 223 U.S. 605, 620, 621-22 (1912) (explaining that "in case of an injury threatened by his illegal action, the officer cannot claim immunity from injunction process. . . . [when] acting in excess of his authority," and that "there may exist ground for equitable relief, when an officer, insisting that he has the warrant of the statute, is transcending its bounds, and thus unlawfully assuming to exercise the power of government against the individual"). For example, in *Harmon v. Brucker*, the Secretary of the Army had issued dishonorable discharges to the plaintiffs based on conduct occurring before their military service began. 355 U.S. at 580. Because the Secretary's statutory authority limited his power to issue dishonorable discharges to instances of dishonorable conduct occurring during military service, the Secretary's actions were in excess of his authority and the plaintiffs were entitled to injunctive relief directing the Secretary to issue them honorable discharges. *Id.* at 582-83.

While *Larson* is recognized as setting the legal standard in this area, the plaintiff in *Larson* failed the test set out by the Supreme Court. In contrast to the situation here, in *Larson* the plaintiff's allegations "were not based and did not purport to be based upon any lack of delegated power." *Larson*, 337 U.S. at 691. The plaintiff sued a government officer seeking specific performance of a government contract, but the officer "had the power and the duty to construe such contracts and to refuse delivery in cases in which he believed that the contract

terms had not been complied with. His action in so doing in [*Larson*] was, therefore, within his authority . . . ." *Id.* at 703. Because the plaintiff did not allege any *ultra vires* acts by the officer, sovereign immunity protected the officer.

Here, Plaintiffs' complaint does allege *ultra vires* acts by the Government Officer Defendants, *i.e.*, a program of dragnet surveillance that the officers lack any power to conduct and that reaches far beyond the narrow statutory limits Congress has imposed on them in the Wiretap Act, ECPA, and FISA. The complaint alleges the factual details of the dragnet content and records surveillance program and explains Defendants' control of and participation in the program. Complaint ¶¶ 7-11, 39-49, 50-81, 82-97. On the basis of these factual allegations, Counts V, VII, X, and XIII allege that by participating in the dragnet surveillance program Government Officer Defendants Alexander, Holder, and Blair have acted in excess of their statutory authority, exceeding the limits that the Wiretap Act, ECPA, and FISA place on their authority. Complaint ¶¶ 76-79, 92-95, 150-51, 154-55, 177, 181-82, 214, 218-19, 237, 241-42. For example, the complaint alleges that "[b]y the acts alleged herein, Defendants acting in excess of their statutory authority . . . have intentionally engaged in . . . electronic surveillance . . . not authorized by any statute" and that "by the acts alleged herein, Defendants acting in excess of their statutory authority and in violation of statutory limitations have intentionally disclosed or used information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance not authorized by statute." Complaint ¶¶ 150-51.

Further reinforcing the express statutory limits that the Wiretap Act, ECPA, and FISA impose on the Government Officer Defendants' conduct is Congress's command that those statutes are the "exclusive means" by which government officers may intercept or conduct electronic surveillance of domestic communications. 18 U.S.C. § 2511(2)(f); 50 U.S.C. § 1812(a). Counts V, VII, X, and XIII, are proper *ultra vires* claims as to which sovereign immunity does not attach, because they allege each "officer's lack of delegated power" rather than "error in the exercise of that power." *See Larson*, 337 U.S. at 689-690.

Nor do the statutes Defendants cite foreclose equitable relief against federal officers for

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

Defendants' reliance on Quiet Title Act decisions to argue that Congress has forbidden Plaintiffs' *ultra vires* claims is equally ill-founded. *See* Gov't Br. at 9 (citing *Block v. N.D.*, 461 U.S. 273 (1983), and *Alaska v. Babbitt*, 75 F.3d 449 (9th Cir. 1996)). In the Quiet Title Act, Congress specifically intended to preclude *ultra vires* suits seeking a judgment depriving the United States of title to real property.[4] *Block*, 461 U.S. at 281-86. Congress expressed no similar intent here.

Defendants' argument that Congress made only a limited waiver of sovereign immunity in 18 U.S.C. § 2712 and by doing so forbade *ultra vires* suits also lacks merit. Because *ultra vires* suits are not suits against the United States and do not require a waiver of sovereign immunity, a partial waiver of sovereign immunity against the United States does not demonstrate an intent to preclude *ultra vires* suits against federal officers who exceed the limits of their statutory authority.

Defendants also err in contending that compelling a federal officer to remain within the limits of his or her statutory authority interferes with the public administration. There is no public interest in unauthorized, lawless conduct by federal officials, and preventing lawless

[4] Such a suit would not be a true *ultra vires* claim in any event, for its purpose would not be to obtain an *in personam* judgment against an officer confining his actions within the limits of his statutory authority, but an *in rem* judgment depriving the United States of its claimed property interest. In such suits, the plaintiff does not assert that the officer lacks statutory authority to deal with the government's real property, but asserts only that the government lacks title to the property over which the officer exercises authority.

conduct advances, rather than interferes with, the public administration. Rather, in a "suit against a public official who invades a private right . . . by exceeding his authority," the Supreme Court has recognized that "relief against the offending officer could be granted without risk that the judgment awarded would '. . . interfere with the public administration.' " *Williams v. Fanning*, 332 U.S. 490, 493 (1947). In *Dugan v. Rank*, 372 U.S. 609, 620-22 (1963), the Supreme Court reaffirmed that *Larson ultra vires* actions are "exceptions to the . . . general rule" regarding suits that might "interfere with the public administration," and remain outside the scope of sovereign immunity.

Finally, *Pennhurst State School & Hospital v. Halderman*, 465 U.S. 89 (1984), has no application here. That case involved efforts to obtain injunctive relief against *state*, not federal, officials to enforce *state*, not federal, law. In that context, the Supreme Court held that a federal court could not intrude upon state sovereignty by enjoining state officials for their failure to operate a state hospital for the mentally retarded in a manner that met state standards of care. *Pennhurst,* 465 U.S. at 106. The federalism, Eleventh Amendment, and Supremacy Clause questions involved in determining the circumstances under which a federal court can impinge on state sovereignty by ordering injunctive relief against state officers do not apply in actions like this one alleging *ultra vires* conduct by federal officers. In any event, *Pennhurst* distinguished *ultra vires* claims from claims that an officer has acted improperly but within the scope of his or her authority. Only the latter are suits against the sovereign with the potential to interfere with the public administration, thus requiring a waiver of sovereign immunity, and only the latter were present in *Pennhurst*. *Id.* at 101 n.11. 11. Here, by contrast, Plaintiffs seek relief against the Government Officer Defendants for acting in excess of their statutory authority. Thus, *Pennhurst* did not and could not have overruled or limited *Larson* as Defendants erroneously suggest.[5]

---

[5] Nor do the other cases Defendants cite support their contention that Plaintiffs' *ultra vires* claims are barred by sovereign immunity. *Central Reserve Life Insurance Co. v. Struve*, 852 F.2d 1158, 1160-61 (9th Cir. 1988), was a case seeking to enforce state law against state officials, and thus was barred by *Pennhurst.* In *Aminoil U.S.A., Inc. v. California State Water Resources Control Board*, 674 F.2d 1227, 1234 (9th Cir. 1982), the Ninth Circuit found that the challenged conduct was within the federal official's statutory authority and not *ultra vires.*

2. Congress waived sovereign immunity for Plaintiffs' equitable relief claims, including Plaintiffs' APA claim.

Section 702 of the Administrative Procedures Act waives sovereign immunity for claims against government agencies and officers seeking equitable relief. 5 U.S.C. § 702. Section 702's waiver applies both to claims brought under section 704 or other provisions of the APA and to claims brought outside the APA to enforce other statutory or constitutional provisions. *Trudeau v. FTC*, 456 F.3d 178, 186 (D.C. Cir. 2006) (holding section 702's "'waiver of sovereign immunity applies to any suit whether under the APA or not'"; quoting *Chamber of Commerce*, 74 F.3d at 1328); *Presbyterian Church (U.S.A.) v. U. S.*, 870 F.2d 518, 525 (9th Cir. 1989) (explaining "§ 702 waives sovereign immunity in all actions seeking relief from official misconduct"); *Assiniboine & Sioux Tribes v. Bd. of Oil & Gas*, 792 F.2d 782, 793 (9th Cir. 1986) (same).

Thus, section 702's waiver applies to Count XVI, which seeks equitable relief under the APA against the government agency Defendants (the United States, the Department of Justice, and the NSA) and against Government Officer Defendants Alexander, Holder, and Blair for constitutional and statutory violations.[6] Section 702 also waives any possible sovereign immunity defense to Counts V, VII, X, and XIII (even though, for the reasons stated in the preceding section, there is no sovereign immunity defense to those claims and thus no need for a waiver). *Trudeau*, 456 F.3d at 186; *Presbyterian Church*, 870 F.2d at 525.

Defendants do not contest that Plaintiffs' APA claim in Count XVI is proper as to the constitutional violations alleged. They contend, however, that section 702's waiver does not apply to Plaintiffs' APA claim in Count XVI to the extent it alleges violations of the Wiretap Act, ECPA, and FISA. In support of that contention, Defendants rely on an exception to section 702's sovereign immunity waiver that applies "if any other statute that grants consent to suit

---

Palomar Pomerado Health System v. Belshe, 180 F.3d 1104, 1108 (9th Cir. 1999), was a suit against state officials with no allegation of *ultra vires* conduct.

[6] Defendants spawn a red herring when they assert that there is no jurisdiction for claims arising under the APA. The general federal question statute, 28 U.S.C. § 1331, gives this Court jurisdiction over actions arising under section 704 or other provisions of the APA. *Califano v. Sanders*, 430 U.S. 99, 106-07 (1977); *Trudeau*, 456 F.3d at 185.

expressly or impliedly forbids the relief which is sought." 5 U.S.C. § 702.

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

Defendants offer four statutes as candidates. The first two statutes that Defendants rely on with respect to the Wiretap Act and ECPA violations, 18 U.S.C. §§ 2520(a) and 2707(a), do not grant consent to suit against the United States, so they do not meet the first requirement of the exception. The third statute, section 2712, does grant consent to suit against the United States, but it does not meet the second requirement because it does not forbid equitable relief. Section 2712 provides that it is "the exclusive remedy against the United States for any claims *within the purview* of this section." 18 U.S.C. § 2712(d) (emphasis added). The purview of section 2712 is set forth in subsection (a) as "an action . . . against the United States to recover money damages." Section 2712 sets the parameters regarding those damages claims, such as requiring the claims to be in excess of $10,000 and making available litigation costs as an additional remedy. 18 U.S.C. § 2712. Thus, only damages claims, and not equitable relief claims, are "within the purview" of section 2712. Section 2712 therefore provides the exclusive avenue for monetary relief and forbids any other claim for money damages, but does not forbid equitable relief.

Finally, contrary to Defendants' argument, the Wiretap Act and EPCA are not similar to the Quiet Title Act, which does preclude APA actions. In *Block*, discussed above, the Supreme Court addressed whether the Quiet Title Act met the terms of section 702's exception to its sovereign immunity waiver. The Quiet Title Act, while granting consent to suit, expressly forbade the very relief the plaintiff in *Block* sought—a judgment awarding it title to a parcel of real property in which the United States had first asserted title more than 12 years previously. *Block*, 461 U.S. at 275 n.1, 286 n.22, n.23. Because the Quiet Title Act both granted consent to suit and expressly forbade the relief the plaintiff sought, it satisfied the terms of the exception to section 702. *Id.* at 286 n.22. By contrast, nothing in the Wiretap Act or ECPA forbids the

equitable relief Plaintiffs seek for violations of those statutes.

Nor do Defendants point to any legislative history or other evidence that Congress intended to forbid equitable relief under the APA for violations of the Wiretap Act and ECPA. With respect to Plaintiffs' APA claim based on FISA violations, 50 U.S.C. § 1810 authorizes damages claims against the United States but does not forbid equitable relief, and does not claim to be the only available remedy. Nor does the Tucker Act support Defendants' contention that section 1810 forbids equitable relief under the APA. The Tucker Act provides a damages remedy for contract claims against the United States. The Tucker Act and its predecessors have been understood for over 150 years, since long before the APA, to prohibit equitable relief for contract claims against the United States; Congress stated that it intended this preexisting understanding to continue when it enacted APA section 702's sovereign immunity waiver in 1976. *United States v. King*, 395 U.S. 1, 3 (1969); *North Side Lumber Co. v. Block*, 753 F.2d 1482, 1485 (9th Cir. 1985).

When Congress enacted FISA in 1978, after section 702's enactment, it did not suggest (as it did with the Tucker Act) that it intended the statutory limits of FISA to be unenforceable by the courts. To the contrary, Congress provided that FISA, the Wiretap Act, and ECPA are the exclusive means by which electronic surveillance may be conducted. 18 U.S.C. § 2511(2)(f); 50 U.S.C. § 1812(a); *Al-Haramain*, 564 F. Supp. 2d at 1116-17, 1121-23. Congress's command that surveillance may only be conducted if it conforms with the narrow limitations of those three Acts would be illusory if judicial review were unavailable to enjoin violations of those Acts by the Executive. *See Al-Haramain*, 564 F. Supp. 2d at 1121 ("When Congress acts to contravene the president's authority, federal courts must give effect to what Congress has required.").

II. For purposes of Plaintiffs' claims, FISA preempts the common-law state secrets privilege.

Defendants' invocation of the state secrets privilege cannot defeat any of Plaintiffs' claims. Congress's detailed, comprehensive FISA protocol governing court review of surveillance-related evidence preempts the common-law state secrets privilege as to the materials underlying Plaintiffs' claims here, and will permit the Court to evaluate all necessary evidence.

A. Where section 1806(f) applies, it preempts the common-law state secrets privilege.

As the Court correctly concluded in *Al-Haramain*, the FISA framework leaves no room for the common-law state secrets privilege to cover materials related to electronic surveillance. *See* 564 F. Supp. 2d at 1118-19; Gov't Br. at 24-25 (raising no new arguments against preemption). Rather, 50 U.S.C. § 1806(f) clearly and comprehensively addresses the proper evidentiary use of allegedly secret materials related to government electronic surveillance, preempting the state secrets privilege for all evidence to which section 1806(f)'s protocol applies. *Al-Haramain*, 564 F. Supp. 2d at 1118-19.

FISA created a detailed statutory framework specifically designed to restrain abuses of executive power and to balance legitimate national security interests with civil liberties in matters related to surveillance. *Id.* at 1115-16. As the Court explained in detail in *Al-Haramain*, section 1806(f) is part of a comprehensive regulatory program that "leaves no room in a case to which section 1806(f) applies" for the common-law state secrets privilege. *Id.* at 1118-19. Rather, section 1806(f) "is Congress's specific and detailed prescription for how courts should handle claims by the government that the disclosure of material relating to or derived from electronic surveillance would harm national security." *Id.* at 1119. Indeed, it "is in effect a codification" of the common law privilege for cases where section 1806(f) applies, "as modified to reflect Congress's precise directive to the federal courts for the handling of materials and information with purported national security implications." *Id.* Accordingly, where it applies, section 1806(f)'s protocol is mandatory—the courts "shall" conduct the review section 1806(f) prescribes in cases within its scope. *Id.* at 1119.

Because section 1806(f)'s plain text directly and clearly addresses the same evidentiary issue as the common-law state secrets privilege, its codified protocol for review of purportedly secret materials related to electronic surveillance replaces the common-law state secrets privilege for all evidence subject to section 1806(f).[7] *Id.* at 1119 (holding that the usual state secrets protocol "has no role where section 1806(f) applies"); 50 U.S.C. § 1806(f); *Kasza v. Browner*,

[7] This result is correct for all the reasons stated in more detail in the Court's *Al-Haramain* decision.

133 F.3d 1159, 1167 (9th Cir. 1998) (discussing preemption of the common-law privilege). That preemption also causes no constitutional concern, because the state secrets privilege is a common-law evidentiary device, not an exclusive constitutional power of the executive. *Al-Haramain*, 564 F. Supp. 2d at 1120; *Mohamed v. Jeppesen Dataplan, Inc.*, 563 F. 3d 992, 1005 (9th Cir. 2009); *Al-Haramain v. Bush,* 507 F.3d 1190, 1196 (9th Cir. 2007) ("*Al-Haramain II*") ("The state secrets privilege is a common law evidentiary privilege"); *see also S.E.C. v. Nacchio*, __ F. Supp. 2d __, 2009 WL 690306 (D. Colo. Mar. 13 2009) ("The State Secrets Privilege is a common-law evidentiary privilege"). Rather, as this Court explained in *Al-Haramain*, Congress has at least equal authority to regulate these matters, even though national security is at issue. 564 F. Supp. 2d at 1120-21. Congress exercised that authority by enacting FISA's section 1806 protocol—as it has done by enacting many other statutes affecting national security and classified information—and the executive and judicial branches must respect the resulting limitations on executive authority. *Id.* at 1121-22 (citing *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U. S. 579 (1952), and numerous statutes).

B. FISA's section 1806(f) procedure applies to the evidence supporting all of Plaintiffs' claims.

FISA's procedure for judicial review of surveillance-related evidence applies to all of the purportedly secret materials underlying Plaintiffs' claims here, and preempts the state secrets privilege for all of those materials. *See Al-Haramain*, 564 F. Supp. 2d at 1119.

By its plain language, section 1806(f) and its preemptive effect apply in any kind of civil or criminal litigation, whether claims are filed under FISA or any other law, when purportedly secret materials related to electronic surveillance are at issue. Specifically, section 1806(f)'s procedures apply "whenever any motion or request" is made by an aggrieved person "pursuant to *any other statute or rule* of the United States or of any State . . . to discover or obtain . . . materials relating to electronic surveillance."[8] 50 U.S.C. § 1806(f) (emphasis added). This

[8] As alleged in detail in the Complaint, Plaintiffs are aggrieved parties under section 1806(f). As in the *Hepting* case, where the Court found that the plaintiffs had adequately alleged standing, Plaintiffs allege a "dragnet" that collected Plaintiffs' communications and records along with those of many other AT&T customers. *See Hepting v. AT&T Corp.*, 439 F. Supp. 2d at 974, at 1000 (N.D. Cal. 2006); Complaint ¶¶ 52-82. *See also* Oct. 16, 2008 Rule 1006 Summary of

language "addresses a range of circumstances in which information derived from electronic surveillance might become relevant to judicial proceedings," not merely the narrow categories of proceedings Defendants suggest. *Al-Haramain*, 564 F. Supp. 2d at 1119. Thus, as this Court concluded in *Al-Haramain*, "section 1806(f) is not limited to criminal proceedings, but may also be invoked in civil actions." *Id.* at 1133; *see also* H.R. Conf. Rep. No. 95-1720 at 32 (1978), *reprinted in* 1978 U.S.C.C.A.N. 4048, 4061 (stating section 1806(f) "is appropriate for determining the lawfulness of electronic surveillance in both criminal and civil cases"). In addition, Congress has further confirmed that section 1806(f)'s procedures apply broadly to surveillance-related evidence in any type of proceeding, by expressly acknowledging the "exclusive" applicability of section 1806(f)'s procedures in actions under other statutes, and declining to create additional, separate review procedures. *See* 18 U.S.C. § 2712(b)(4) (expressly confirming that in actions against the United States under section 2712, including claims under ECPA and the Wiretap Act, section 1806(f)'s procedures "shall be the exclusive means" for reviewing materials subject to section 1806(f)).

As in *Hepting*, which involved the same underlying facts as this case, the gravamen of all of Plaintiffs' claims here is that the government and private telecommunications companies like AT&T have created an illegal, comprehensive "dragnet that collects the content and records of [AT&T's] customers' communications." *Hepting*, 439 F. Supp. 2d at 978, 1000. *See, e.g.*, Complaint ¶¶ 60-97 (generally describing the same illegal surveillance scheme), 143-167 (specifically alleging "electronic surveillance" of Plaintiffs' communications in violation of FISA). All of Plaintiffs' claims are related to that illegal surveillance dragnet, as is all of the purportedly secret evidence that will be before the Court. For example, all materials concerning the government's collection of communications records are at a minimum "materials relating to electronic surveillance" under section 1806(f) because those records are used as part of the government's targeting process to decide which communications will receive additional scrutiny from government analysts. *See* Complaint ¶ 11. Thus, section 1806(f)'s protocol preempting the

---

Evidence (MDL No. 1791, Docket No. 481; Exh. A to Plaintiffs' accompanying Rule 56(f) Declaration) (summarizing voluminous public evidence supporting Plaintiffs' claims).

state secrets privilege permits—and requires—the Court to evaluate the surveillance-related materials underlying Plaintiffs' factual allegations, and all of the causes of action arising out of them.

Because section 1806(f) preempts the state secrets privilege and expressly authorizes the Court to review the surveillance-related materials at issue in this case, with appropriate security protections, Plaintiffs' claims cannot be dismissed at any stage on the basis of the state secrets privilege. More fundamentally, no evidence can be excluded from this litigation at this time on the basis of the state secrets privilege. *See infra.* Instead, section 1806(f)'s protocol will permit the Court to evaluate whatever evidence is necessary to decide Plaintiffs' claims on their merits, at the appropriate time.

III. Even if the state secrets privilege were not preempted, this case could not be dismissed based on the privilege.

Because section 1806(f) preempts the state secrets privilege, Defendants' argument that the state secrets privilege requires dismissal fails and the Court need not consider it further. Even if section 1806(f) did not preempt the state secrets privilege, however, the state secrets privilege would still provide no basis for dismissing this action, as the Ninth Circuit recently confirmed in *Mohamed,* 563 F.3d at 1004.

A. The narrow "very subject matter" litigation bar is limited to secret agreements between a plaintiff and the executive, and does not apply here.

In *Mohamed*, the Ninth Circuit reaffirmed that threshold dismissal of an action because its "very subject matter" is a state secret is permissible only if the case is based on a secret agreement between the plaintiff and the government:

> [I]f a lawsuit is not predicated on the existence of a secret agreement between the plaintiff and the government, *Totten* [*v. United States*, 92 U.S. 105 (1875)] does not apply and the subject matter of the suit is not a state secret.

563 F.3d at 1004. Here, there is no agreement, secret or otherwise, between Plaintiffs and the government. *See Hepting*, 439 F. Supp. 2d at 991 ("[P]laintiffs made no agreement with the government and are not bound by any implied covenant of secrecy.") Accordingly, the subject matter of this suit is not a state secret and the suit may not be dismissed at the outset.

Mohamed was a suit brought against a government contractor by alleged victims of the

CIA's extraordinary rendition program. "[T]he government argue[d]," as it does here, "that state secrets form the subject matter of a lawsuit, and therefore require dismissal, any time a complaint contains allegations, the truth or falsity of which has been classified as secret by a government official." *Mohamed*, 563 F.3d at 1003. The Ninth Circuit categorically rejected this argument:

> This sweeping characterization of the "very subject matter" bar has no logical limit—it would apply equally to suits by U.S. citizens, not just foreign nationals; and to secret conduct committed on U.S. soil, not just abroad. According to the government's theory, the Judiciary should effectively cordon off all secret government actions from judicial scrutiny, immunizing the CIA and its partners from the demands and limits of the law.

Id. The Ninth Circuit held that, instead of threshold dismissal, the proper course is for a court to consider assertions of the state secrets privilege on an item-by-item basis under *Reynolds*: "Unlike *Totten*, the *Reynolds* framework accommodates these division-of-powers concerns by upholding the President's secrecy interests without categorically immunizing the CIA or its partners from judicial scrutiny." *Id.* at 1004.

The exact concerns raised by the Ninth Circuit exist here—the government is seeking dismissal of a suit brought by United States citizens about secret conduct on United States soil and seeks to immunize itself from the "demands and limits of the law." *See id.* at 1003. As in *Mohamed*, application of the *Reynolds* framework—if the Court were to find it not preempted here by section 1806(f)—is the only way to ensure that the secrecy interests of the President are upheld without categorically immunizing the government from judicial scrutiny.[9] *Id.*

B. Defendants cannot dismiss this suit based on their speculative contention that future state secrets assertions will prevent presentation of evidence needed for Plaintiffs' prima facie case or Defendants' defenses.

Mohamed also disposed of Defendants' argument that threshold dismissal is appropriate because Defendants predict that Plaintiffs cannot establish standing or other elements of their prima facie case, or that Defendants cannot defend themselves, without using evidence that is protected by the state secrets privilege.

---

[9] Even without relying on *Mohamed*, this Court's *Hepting* decision confirms that the very subject matter of this action is not a state secret. This action and *Hepting* arise from a common factual basis and share a common subject matter. This Court already held in *Hepting* that the very subject matter is not a state secret. *Hepting*, 439 F. Supp. 2d at 994; *see also Al Harimain II*, 507 F.3d at 1201. Because *Hepting* and this action share a common subject matter, the specific

The Ninth Circuit firmly rejected the troubling proposition that courts may anticipatorily dismiss cases by applying the state secrets privilege prior to any concrete evidentiary dispute over a specific item of evidence: "[N]either the Federal Rules nor *Reynolds* would permit us to dismiss this case at the *pleadings stage* on the basis of an evidentiary privilege that must be invoked during *discovery* or *at trial*." *Mohamed*, 563 F.3d at 1009 (emphases in original). Instead, the Ninth Circuit articulated a clear framework for evaluating state secret privilege claims, grounded in fundamental Article III and separation-of-powers principles. It held that courts—not the Executive Branch—must exercise "control over the evidence in a case." *Id.* at 1001 (quoting *Reynolds*, 345 U.S. at 9-10); *Mohamed*, 563 F.3d. at 1004 ("Separation-of-powers concerns take on an especially important role in the context of secret Executive conduct."). Under this framework, before deciding whether or how the state secrets privilege applies to a particular item of evidence, the court must await:

> (1) an actual request for discovery of specific evidence,
> (2) an explanation from plaintiffs of their need for the evidence, and
> (3) a formal invocation of the privilege by the government with respect to that evidence, explaining why it must remain confidential.

Id. at 1008-1009 (citations omitted). "[R]ather than foreclosing litigation altogether at the outset," the court then "excis[es] secret evidence on an item-by-item basis." *Id.* at 1003-1004.

Previously, this Court reached the same conclusion in *Hepting*. There, the Court held that "it would be premature to conclude that the [state secrets] privilege will bar evidence necessary for plaintiffs' *prima facie* case or AT&T's defense," *Hepting,* 439 F. Supp. 2d at 994, and rejected the argument that "plaintiffs' claims would necessarily lack the factual support required to withstand a future jurisdictional challenge based on lack of standing," *id.* at 1001.

In short, a court may not dismiss a lawsuit based on the government's presumption that its future assertions of the state secrets privilege in response to as-yet unknown discovery requests will leave the plaintiffs unable to establish their claims or the defendants unable to prove their defenses. In *Mohamed*, for example, the government argued that victims of the CIA's "extraordinary rendition" program could not maintain their lawsuit because the plaintiffs

---

subject matter of this action also is not a state secret.

could not establish a prima facie case, or the defendants could not defend themselves, without using privileged evidence. The Court held:

> We are unpersuaded because acceding to the government's request would require us to ignore well-established principles of civil procedure. At this stage of the litigation we simply cannot prospectively evaluate hypothetical claims of privilege that the government has not yet raised and the district court has not yet considered.

Mohamed, 563 F.3d at 1008; *accord Al-Haramain II*, 507 F.3d at 1203 ("Simply saying 'military secret,' 'national security' or 'terrorist threat' or invoking an ethereal fear that disclosure will threaten our nation is insufficient to support the privilege."); *id.* at 1201 (explaining that "the decision on the state secrets privilege may need to await preliminary discovery").[10]

Mohamed also laid to rest an argument that permeates the government's motions to dismiss in both this case and in *Hepting*. In *Mohamed*, as here, the government argued that the state secrets privilege protected information rather than evidence. The *Mohamed* Court rejected this argument:

> Outside of the extremely narrow *Totten* context, the state secrets privilege has never applied to prevent parties from litigating the truth or falsity of allegations, or facts, or information simply because the government regards the truth or falsity of the allegations to be secret . . . According to *Reynolds,* therefore, the question is not which *facts* are secret and may not be alleged and put to the jury's consideration for a verdict; it is only which *evidence* is secret and may not be disclosed in the course of a public trial. [¶] . . . [T]he privilege applies to prevent discovery of the evidence itself and not litigation of the truth or falsity of the information that might be contained within it.

563 F.3d at 1005 (emphases in original). Among other things, this means that the state secrets privilege cannot be "invoked to prevent a litigant from persuading a jury of the truth or falsity of an allegation by reference to non-privileged evidence, regardless whether privileged evidence might also be probative." *Id.*

---

[10] *Al-Haramain II* also helps refute the circular claim that the Court must dismiss based on lack of standing before it reviews critical evidence that could establish standing. In *Al-Haramain II*, the Ninth Circuit noted that it "read *Reynolds* as requiring *in camera* review" of the critical evidence in *Al-Haramain II* required to establish standing (the Sealed Document). The Ninth Circuit relied on "Al-Haramain's admittedly substantial need for the document to establish its case." *Id.* at 1203 (citation omitted). To the extent that Defendants claim that Plaintiffs need secret evidence to establish standing (which Plaintiffs deny), Plaintiffs would have a similar "substantial need" for that evidence here.

Under *Mohamed*, therefore, Defendants' invocation of the state secrets privilege here is defective for two reasons: first, because Defendants invoke the privilege prematurely in advance of any discovery request by Plaintiffs, and, second, because they invoke it by contending that certain facts and information are secret and cannot be litigated, rather than contending that specific items of evidence are secret.

As to the first flaw, *Mohamed* makes clear that Defendants must await specific discovery requests from Plaintiffs. Only after those requests are presented, and then only if Defendants assert the state secrets privilege with respect to specific items of evidence responsive to Plaintiffs' requests, may this Court decide whether the privilege bars admission of a specific item of evidence.

As to the second flaw, each of Defendants' specific assertions of privilege is improperly directed at facts and information rather than specific items of evidence. For example, Defendants improperly attempt to assert the state secrets privilege over the following:

> B. Information that may tend to confirm or deny whether the plaintiffs have been subject to any alleged NSA intelligence activity that may be at issue in this matter; and
>
> C. Any information concerning NSA intelligence activities, sources or methods that may relate to or be necessary to litigate plaintiffs' allegations, including allegations that the NSA, with the assistance of telecommunications carriers such as AT&T, indiscriminately intercepts the content of communications and also collects the communications of millions of Americans. . . includ[ing] but not limited to:
>
> (i) Information concerning the scope and operation of the now inoperative "Terrorist Surveillance Program," . . .
>
> (ii) Information concerning whether or not the NSA obtained from telecommunications companies such as AT&T communication transactional records as alleged in the Complaint … ;
>
> (iii) Information that may tend to confirm or deny whether AT&T (and to the extent relevant or necessary, any other telecommunications carrier), has provided assistance to the NSA in connection with any alleged activity."

Dir. of Nat'l Intel. Blair's Public Decl. (Docket No. 18-3) ¶¶ 11, 13-18; Bonnani Public Decl. (Docket No. 18-4), ¶¶ 10-16 ("supporting" the DNI's state secrets privilege assertion). These conclusory attempts to claim privilege over all facts and information needed for Plaintiffs to succeed in their claims (whether secret or not), rather than over specific items of evidence

requested by Plaintiffs, are inadequate under *Mohamed.*

Finally, the Ninth Circuit made clear that threshold dismissal is inappropriate even if the government successfully establishes that particular items of evidence are covered by the state secrets privilege. A court cannot "determine whether the parties will be able to establish their cases without use of privileged evidence without also knowing what *non-privileged* evidence they will marshal." *Mohamed*, 563 F.3d at 1009 (emphasis in original) (citing *Crater Corp. v. Lucent Technologies, Inc.*, 423 F.3d 1260, 1267-68 (Fed. Cir. 2005), for proposition that "deciding the impact of the government's assertion of the state secrets privilege" before the record is "adequately developed" puts "the cart before the horse").

This holding is especially applicable here because four of these same Plaintiffs have already presented a large and compelling body of undisputed, unprivileged evidence about the surveillance dragnets in *Hepting* and in the related Multi-District Litigation, *In re National Security Agency Telecommunication Records Litigation* (Case No. M:06-cv-01791-VRW), the existence of which this Court may judicially notice.[11] Thus, even if Defendants' invocation of the state secrets privilege were not premature and defective, in addition to being preempted here by 50 U.S.C. §1806(f), it would still provide no basis for dismissal of this action.

//

//

[11] Additionally, Plaintiffs file herewith a Declaration pursuant to Fed. R. Civ. Pro. 56(f) outlining additional discovery that they would conduct which would support their Opposition should Defendants' motion be deemed a motion for summary judgment.

CONCLUSION

For all the foregoing reasons, Defendants' Motion to Dismiss should be denied.

Respectfully submitted,

Dated: June 3, 2009

By: /s/

ELECTRONIC FRONTIER FOUNDATION
CINDY COHN (SBN 145997)
LEE TIEN (SBN 148216)
KURT OPSAHL (SBN 191303)
KEVIN S. BANKSTON (SBN 217026)
JAMES S. TYRE (SBN 083117)
454 Shotwell Street
San Francisco, California 94110
Telephone: (415) 436-9333
Facsimile: (415) 436-9993

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

RICHARD R. WIEBE (SBN 121156)
LAW OFFICE OF RICHARD R. WIEBE
425 California Street, Suite 2025
San Francisco, California 94104
Telephone: (415) 433-3200
Facsimile: (415) 433-6382

THOMAS E. MOORE III (SBN 115107)
THE MOORE LAW GROUP
228 Hamilton Avenue, 3rd Floor
Palo Alto, California 94301
Telephone: (650) 798-5352
Facsimile: (650) 798-5001

Attorneys for Plaintiffs