CASE NO. 19-16066
(PRIOR APPEALS: NOS. 10-15616, 15-16133)

IN THE UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT

CAROLYN JEWEL, TASH HEPTING, ERIK KNUTZEN, YOUNG BOON HICKS (AS EXECUTRIX OF THE ESTATE OF GREGORY HICKS), AND JOICE WALTON,

PLAINTIFFS-APPELLANTS,

V.

NATIONAL SECURITY AGENCY, *ET AL.*,

DEFENDANTS-APPELLEES.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF CALIFORNIA, NO. 08-CV-04373-JSW
THE HONORABLE JEFFREY S. WHITE, UNITED STATES DISTRICT JUDGE, PRESIDING

APPELLANTS' EXCERPTS OF RECORD
Vol. 1 of 8, Pages ER 001 to ER 081

RACHAEL E. MENY
BENJAMIN W. BERKOWITZ
PHILIP J. TASSIN
KEKER, VAN NEST & PETERS LLP
633 Battery Street
San Francisco, CA 94111
Telephone: (415) 391-5400

THOMAS E. MOORE III
ROYSE LAW FIRM, PC
149 Commonwealth Drive, Suite 1001
Menlo Park, CA 94025
Telephone: (650) 813-9700

ARAM ANTARAMIAN
LAW OFFICE OF ARAM ANTARAMIAN
1714 Blake Street
Berkeley, CA 94703
Telephone: (510) 841-2369

RICHARD R. WIEBE
LAW OFFICE OF RICHARD R. WIEBE
44 Montgomery Street, Suite 650
San Francisco, CA 94104
Telephone: (415) 433-3200

CINDY A. COHN
DAVID GREENE
LEE TIEN
KURT OPSAHL
ANDREW CROCKER
JAMIE L. WILLIAMS
AARON MACKEY
JAMES S. TYRE
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333

Counsel for Plaintiffs-Appellants

APPELLANTS' EXCERPTS OF RECORD

INDEX

(ECF Numbers are from N.D. Cal. No. 08-CV-04373-JSW.)

84-2	7/2/12	Declaration of Mark Klein	**ER 1206**
84-3	7/2/12	**Exhibit A** (under seal unredacted version)	**ER 1216**
84-4	7/2/12	**Exhibit B** (under seal unredacted version)	**ER 1260**
84-5, 84-6	7/2/12	**Exhibit C** (under seal unredacted version)	**ER 1281**

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

CAROLYN JEWEL, ET AL.,

Plaintiffs,

v.

NATIONAL SECURITY AGENCY, ET AL.,

Defendants.
_____/

No. C 08-04373 JSW

JUDGMENT

Pursuant to the Court's Order granting the motion for summary judgment filed by Defendants National Security Agency, United States, Department of Justice, Paul M. Nakasone, Donald J. Trump, William Barr, and Daniel Coats, in their official capacities (collectively, "Defendants") and DENYING the cross-motion to proceed to resolution on the merits filed by Plaintiffs Carolyn Jewel, Tash Hapting, Young Boon Hicks, as executrix of the estate of Gregory Hicks, Erik Knutzen, and Joice Walton, on behalf of themselves and all other individuals similarly situated ("Plaintiffs") it is HEREBY ORDERED AND ADJUDGED that judgment is entered in favor of Defendants and against Plaintiffs.

IT IS SO ORDERED.

Dated: April 25, 2019

JEFFREY S. WHITE
UNITED STATES DISTRICT JUDGE

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

CAROLYN JEWEL, ET AL.,

Plaintiffs,

v.

NATIONAL SECURITY AGENCY, ET AL.,

Defendants.
_____/

No. C 08-04373 JSW

NOTICE OF FILING OF CLASSIFIED ORDER

The Court hereby provides notice that the Supplemental Classified Order Granting Defendants' Motion for Summary Judgment and Denying Plaintiffs' Cross-Motion, dated April 25, 2019, is being filed *ex parte* under seal with the Court's Classified Information Security Officer and shall be preserved in the Court's sealed record pending any further proceeding.

IT IS SO ORDERED.

Dated: April 25, 2019

JEFFREY S. WHITE
UNITED STATES DISTRICT JUDGE

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

CAROLYN JEWEL, ET AL.,

Plaintiffs,

v.

NATIONAL SECURITY AGENCY, ET AL.,

Defendants.

No. C 08-04373 JSW

ORDER GRANTING DEFENDANTS' MOTION FOR SUMMARY JUDGMENT AND DENYING PLAINTIFFS' CROSS-MOTION

/

Now before the Court is the motion for summary judgment filed by Defendants National Security Agency, United States, Department of Justice, Paul M. Nakasone, Donald J. Trump, William Barr, and Daniel Coats, in their official capacities (collectively, "Defendants") and the cross-motion to proceed to resolution on the merits filed by Plaintiffs Carolyn Jewel, Tash Hapting, Young Boon Hicks, as executrix of the estate of Gregory Hicks, Erik Knutzen, and Joice Walton, on behalf of themselves and all other individuals similarly situated ("Plaintiffs").

Having considered the parties' papers, including Defendants' classified submissions, and the parties' arguments, the Court GRANTS Defendants' motion for summary judgment and DENIES Plaintiffs' cross-motion for summary judgment.

BACKGROUND

A. Factual Procedural Background.

This case is one of many arising from claims that the federal government, with the assistance of major telecommunications companies, conducted widespread warrantless dragnet communications surveillance of United States citizens following the attacks of September 11, 2001. On September 18, 2008, Plaintiffs filed this putative class action on behalf of themselves and a class of similarly situated persons described as "millions of ordinary Americans . . . who use[] the phone system or the Internet" and "a class comprised of all present and future United States persons who have been or will be subject to electronic surveillance by the National Security Agency without a search warrant or court order since September 12, 2001." (Complaint at ¶¶ 1, 7, and 9.) The Court is now faced with the challenge of determining whether, as Plaintiffs describe it, the data and metadata collection programs may violate Plaintiffs' remaining statutory protections afforded them by the Wiretap Act and the Electronic Communications Privacy Act or the Stored Communications Act. Further, the Court is tasked with the preliminary question whether the Plaintiffs may maintain their claims based on the evidence of their standing and the potential that continued litigation may imperil national security.

According to the allegations in the Complaint, a program of dragnet surveillance (the "Program") was first authorized by Executive Order of the President on October 4, 2001. (*Id.* at ¶¶ 3, 39.) Under this Program (and subsequently under statutory authorities) the NSA undertook the collection of non-content telephony and Internet metadata in bulk, and the contents of certain Internet communications. (*See id.* at ¶¶ 3-13, 39; *see also* Dkt. No. 389, Declaration of Michael S. Rogers ("Rogers Decl.") ¶¶ 40, 47-48, 51-52.) Plaintiffs allege that, in addition to eavesdropping on or reading specific communications, Defendants have "indiscriminately intercepted the communications content and obtained the communications records of millions of ordinary Americans as part of the Program authorized by the President." (Complaint ¶ 7.) The core component of the Program is a nationwide network of sophisticated communications surveillance devices attached to the key facilities of various

telecommunications companies that carry Americans' Internet and telephone communications. (*Id.* at ¶¶ 8, 42.) Plaintiffs allege that Defendants have unlawfully solicited and obtained the private telephone and internal transactional records of millions of customers of the telecommunications companies, including records indicating who the customers communicated with, when those communications took place and for how long, among other sensitive information. Plaintiffs allege these records include both domestic and international communications. (*Id.* at ¶ 10.) Plaintiffs sue Defendants "to enjoin their unlawful acquisition of the communications and records of Plaintiffs and class members, to require the inventory and destruction of those that have already been seized, and to obtain appropriate statutory, actual, and punitive damages to deter future illegal surveillance." (*Id.* at ¶ 14.)

Plaintiffs originally alleged seventeen counts against Defendants: violation of the Fourth Amendment (counts 1 and 2); violation of the First Amendment (counts 3 and 4); violation of the Foreign Intelligence Surveillance Act ("FISA"), 50 U.S.C. §§ 1809, 1810 (counts 5 and 6); violation of the Wiretap Act, 18 U.S.C. § 2511(1)(a), (b), and (d) (counts 7 through 9); violation of the Electronic Communications Privacy Act or the Stored Communications Act, 18 U.S.C. § 2703(a), (b), and (c) (counts 10 through 15); violation of the Administrative Procedure Act, 5 U.S.C. § 701 *et seq.* (count 16); and violation of separation of powers (count 17).

After the Complaint was filed on September 18, 2008, Defendants moved to dismiss and alternatively sought summary judgment as to all claims. Defendants argued that the Court lacked jurisdiction over the statutory claims because the Government had not waived its sovereign immunity. Defendants moved for summary judgment on the remaining claims based primarily on the contention that the information necessary to litigate the claims was properly subject to the state secrets privilege.

The district court, the Honorable Vaughn R. Walker presiding, dismissed the claims without leave to amend based on the finding that Plaintiffs had failed to make out the *prima facie* allegations necessary to establish standing. (Dkt. No. 57.)

On appeal, the Ninth Circuit Court of Appeals reversed the district court's dismissal of the Complaint on the ground of lack of standing. The appeals court concluded that, at the pleadings stage, "Jewel [had] alleged a sufficiently concrete and particularized injury. Jewel's allegations are highly specific and lay out concrete harms arising from the warrantless searches." *See Jewel v. National Security Agency*, 673 F.3d 902, 909-10 (9th Cir. 2011). Although the appellate court remanded on the basis that it was premature to dismiss premised upon lack of standing, the court noted that "procedural, evidentiary, and substantive barriers" might ultimately doom Plaintiffs' proof of standing. *See id.* at 911. The court remanded "with instructions to consider, among other claims and defenses, whether the government's assertion that the state secrets privilege bars this litigation." *Id.* at 913-14.

Upon remand, Plaintiffs filed a motion for partial summary adjudication urging the Court to reject Defendants' state secret defense. Defendants cross-moved to dismiss on the basis of sovereign immunity for the statutory claims and for summary judgment on the assertion of the state secrets privilege.

On July 23, 2013, this Court granted Plaintiffs' motion for partial summary adjudication by rejecting the state secrets defense as having been displaced by the statutory procedure prescribed in 50 U.S.C. Section 1806(f) of FISA. (Dkt. No. 153.) The Court granted Defendants' motions to dismiss Plaintiffs' claims for damages under FISA and all statutory claims for injunctive relief on the basis of sovereign immunity. Further, the Court reserved ruling on the Defendants' motions for summary judgment on the remaining non-statutory claims.

On July 25, 2014, Plaintiffs moved for partial summary judgment on their Fourth Amendment claims and on September 29, 2014, Defendants cross-moved on the threshold issue of standing and on the merits of the Fourth Amendment claim. On February 10, 2015, this Court denied Plaintiffs' motion and granted Defendants' motion for partial summary judgment on Plaintiffs' Fourth Amendment claims. (Dkt. No. 321.) Relying on both the public record and Defendants' classified submissions, the Court found that Plaintiffs had failed to establish a sufficient factual basis to assert they had standing to sue under the Fourth Amendment

regarding the possible interception of their Internet communications. Further, the Court found that the Fourth Amendment claim would otherwise have to be dismissed because even if Plaintiffs could establish standing, such a potential claim would have to be dismissed on the basis that any possible defenses would require the impermissible disclosure of state secret information.

On May 20, 2015, this Court granted Defendants' motion for entry of judgment under Federal Rule of Civil Procedure 54(b) on the basis that the threshold issue of standing and its adjudication in the Fourth Amendment context was a final determination and no just reason existed for delay in entering final judgment on the constitutional claim. (Dkt. No. 327.)

Plaintiffs appealed that ruling, and on December 18, 2015, the Ninth Circuit, dismissed the appeal, reversed the certification, and remanded to this Court. (Dkt. No. 333.) The appellate court found that the severable claim of liability under the Fourth Amendment did not encompass all plaintiffs or defendants or all remaining claims and therefore the piecemeal resolution of individual issues did not satisfy the requirements of Rule 54(b). The Ninth Circuit remanded with instructions to expend the parties' and the district court's resources in an effort to obtain a final and comprehensive judgment of this entire matter.

Immediately upon remand, on February 19, 2016, this Court lifted the stay of discovery on the remaining statutory claims and admonished the parties to seek resolution of all remaining matters by summary adjudication on the merits, with the benefit of any potentially available discovery. (Dkt. No. 340.) The Court permitted Plaintiffs to serve discovery requests limited to the issue of their standing to pursue the remaining statutory claims. The Court directed Defendants to file its unclassified objections and responses to Plaintiffs' requests in the public record, and to submit classified documents and information responsive to Plaintiffs' discovery requests *ex parte* and *in camera*. The Court also tasked the Defendants to marshal all evidence bearing on the issue of Plaintiffs' standing, even if it had not been specifically requested by Plaintiffs. (Dkt. No. 356.)

On August 17, 2018, after having reviewed both the classified and public materials produced and in the record, this Court issued an order requiring the parties to file cross motions

for summary judgment on the issue of Plaintiffs' standing or lack of standing as to each of the remaining claims. (Dkt. No. 410.)

The currently pending cross-motions are now ripe for resolution.

B. Legal Framework Background.

In its order dated July 23, 2013, the Court found that, after the Ninth Circuit remanded this Court's order finding that Plaintiffs lacked standing prior to the proffer of discovery, the Court could utilize the statutory procedure prescribed in 50 U.S.C. Section 1806(f) of FISA ("Section 1806(f)") in order to address the ongoing litigation. Further, the Court found that the state secrets defense did not require immediate dismissal of the matter. In that order, the Court found that the use of the procedural mechanism established by Section 1806(f) would not automatically result in the summary exclusion of all potentially classified information. Rather than merely permitting the assertion of the state secrets privilege to result in immediate dismissal of this action, the Court has, on numerous occasions, permitted Defendants to supply classified evidence for the Court's *in camera* review. *See also In re National Security Agency Telecommunications Records Litigation*, 564 F. Supp. 2d 1109, 1111 (N.D. Cal. 2008) ("FISA preempts the state secrets privilege in connection with electronic surveillance for intelligence purposes . . . ."). Having found that Section 1806(f) of FISA displaces the state secrets privilege as a procedural mechanism in cases in which electronic surveillance yields potentially sensitive evidence by providing secure procedures under which courts can consider national security evidence, this Court has determined that the application of the state secrets privilege would not automatically apply to summarily exclude litigation of this action.

Subsequent to this Court's determination that FISA preempts the state secrets privilege in connection with electronic surveillance for intelligence purposes, the Ninth Circuit similarly and more recently concluded that "in enacting FISA, Congress displaced the common law dismissal remedy created by the *Reynolds* state secrets privilege as applied to electronic surveillance within FISA's purview." *Fazaga v. Federal Bureau of Investigation*, 916 F.3d 1202, 1230 (9th Cir. 2019). The court held that the electronic surveillance claims brought by the plaintiffs in that case were "not subject to outright dismissal at the pleading stage," and

remanded so that the district court could employ the procedures established by Section 1806(f) to review evidence over which Defendants had asserted the state secrets privilege. *Id.* at 1226, 1251. This Court has, in the lengthy course of this case, employed those procedures.

Now, having required briefing on the remaining statutory claims and having required the proffer of evidence regarding standing from both Plaintiffs and Defendants, both public and classified, the Court may determine the full extent of the threshold legal issue regarding whether Plaintiffs have standing to sue and the determination, regardless whether Plaintiffs have standing to sue, if the Court may proceed to the merits of this case. As discussed at greater length in Section II of the Court's Supplemental Classified Order Granting Defendants' Motion for Summary Judgment and Denying Plaintiffs' Cross-Motion ("Classified Order") filed herewith, after over ten years of litigation and multiple disclosures, the Court accepts the representation of the Defendants that they are unable to defend the litigation or to pursue it to resolution on the merits without grave risk to the national security.

ANALYSIS

A. Legal Standard on Motion for Summary Judgment.

A principal purpose of the summary judgment procedure is to identify and dispose of factually unsupported claims. *Celotex Corp. v. Cattrett*, 477 U.S. 317, 323-24 (1986). Summary judgment is proper when the "pleadings, depositions, answers to interrogatories, and admissions on file, together with the affidavits, if any, show that there is no genuine issue as to any material fact and that the moving party is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(a). "In considering a motion for summary judgment, the court may not weigh the evidence or make credibility determinations, and is required to draw all inferences in a light most favorable to the non-moving party." *Freeman v. Arpaio*, 125 F.3d 732, 735 (9th Cir. 1997).

The party moving for summary judgment bears the initial burden of identifying those portions of the pleadings, discovery, and affidavits that demonstrate the absence of a genuine issue of material fact. *Celotex*, 477 U.S. at 323; *see also* Fed. R. Civ. P. 56(c). An issue of fact is "genuine" only if there is sufficient evidence for a reasonable fact finder to find for the non-

moving party. *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248-49 (1986). A fact is "material" if it may affect the outcome of the case. *Id.* at 248. Once the moving party meets its initial burden, the non-moving party must go beyond the pleadings and, by its own evidence, "set forth specific facts showing that there is a genuine issue for trial." Fed. R. Civ. P. 56(e).

In order to make this showing, the non-moving party must "identify with reasonable particularity the evidence that precludes summary judgment." *Keenan v. Allan*, 91 F.3d 1275, 1279 (9th Cir. 1996) (quoting *Richards v. Combined Ins. Co.*, 55 F.3d 247, 251 (7th Cir. 1995) (stating that it is not a district court's task to "scour the record in search of a genuine issue of triable fact"); *see also* Fed. R. Civ. P. 56(e). If the non-moving party fails to point to evidence precluding summary judgment, the moving party is entitled to judgment as a matter of law. *Celotex*, 477 U.S. at 323; *see also* Fed. R. Civ. P. 56(e)(3).

B. Legal Standard on Threshold Issue of Standing.

"[T]here can be no genuine issue as to any material fact" where a party "fails to make a showing sufficient to establish the existence of an element essential to that party's case, and on which [it bears] . . . the burden of proof." *Celotex*, 477 U.S. at 322. Standing is "an essential . . . part of the case-or-controversy requirement of Article III." *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992). In order for Plaintiffs to establish Article III standing, they must show they: "(1) suffered injury in fact, (2) that is fairly traceable to the challenged conduct of the [Defendants], (3) that is likely to be redressed by a favorable judicial decision." *Spokeo, Inc. v. Robins*, __ U.S. __, 136 S. Ct. 1540, 1547 (2016) (citing *Lujan*, 504 U.S. at 650-61). Plaintiffs bear the burden of proving the existence of standing to sue. *See, e.g., United States v. Hays*, 515 U.S. 737, 743 (1995). Plaintiffs must be able to establish standing for each claim and for each form of relief. *See, e.g., DaimlerChrysler Corp. v. Cuno*, 547 U.S. 332, 352 (2006); *Davidson v. Kimberly Clark*, 889 F.3d 956, 967 (9th Cir. 2018).

"In other words, plaintiffs here must show *their own* metadata was collected by the government." *Obama v. Klayman*, 800 F.3d 559, 562 (D.C. Cir. 2015) (citations omitted; emphasis in original); *see also Halkin v. Helms*, 690 F.2d 977, 999-1000 (D.C. Cir. 1982) ("[T]he absence of proof of actual acquisition of appellants' communications is fatal to their

watchlisting claims.") Because a demonstration of standing is an "indispensable part of their case," and in order to prevail on their motion for summary judgment, Plaintiffs must support their allegations of standing "in the same way as any other matter on which [they] bear the burden of proof, *i.e.*, with the manner and degree of evidence required at the successive stages of the litigation." *Bras v. Cal. Pub. Utils. Comm'n*, 59 F.3d 869, 872 (9th Cir. 1995) (quoting *Lujan*, 504 U.S. at 561). Plaintiffs must proffer admissible evidence establishing both their standing as well as the merits of their claims. *See* Fed. R. Civ. P. 56(c); *see also In re Oracle Corp. Sec. Litig.*, 627 F.3d 376, 385 (9th Cir. 2010) (holding that the court's ruling on summary judgment must be based only on admissible evidence); *see also Orr v. Bank of America NT & SA*, 285 F.3d 764, 773 (9 th Cir. 2001) (citing Fed. R. Evid. 901(a)) (holding that a trial court may only consider admissible evidence on ruling on a motion for summary judgment and authentication is a "condition precedent to admissibility"). If Plaintiffs are unable to make a showing sufficient to establish an essential element of their claim on which they bear the burden at trial, summary judgment must be granted against them. *See Celotex Corp.*, 477 U.S. at 322.

"To establish Article III Standing, an injury must be 'concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling.'" *Clapper v. Amnesty International USA*, 568 U.S. 398, 409 (2013) ("*Clapper*") (quoting *Monsanto Co. v. Geertson Seed Farms*, 561 U.S. 139, 149 (2010)). "Although imminence is concededly a somewhat elastic concept, it cannot be stretched beyond its purpose, which is to ensure that the alleged injury is not too speculative for Article III purposes – that the injury is *certainly* impending." *Id.* (citing *Lujan*, 504 U.S. at 565 n.2) (emphasis in original). Thus, the Supreme Court has "repeatedly reiterated that 'the threatened injury must be *certainly impending* to constitute injury in fact,' and that '[a]llegations of *possible* future injury' are not sufficient." *Id.* (quoting *Whitmore v. Arkansas*, 495 U.S. 149, 158 (1990) (emphasis in original)).

In order to establish standing on the remaining statutory grounds, Plaintiffs must be able to show that they have suffered an injury in fact that is (1) "concrete [and] particularized," (2) "fairly traceable to the challenged action[s]" of the defendants, and (3) "redressable by a

favorable ruling." *Clapper*, 568 U.S. at 409. In order to demonstrate that Plaintiffs have suffered the requisite injury in fact, Plaintiffs must, using publicly available facts, adduce admissible evidence that the contents of their communications or the metadata regarding those communications were subject to the intelligence-collection activities they challenge in this case. Plaintiffs must demonstrate that they "personally suffered a concrete and particularized injury in connection with the conduct about which [they] complain." *Trump v. Hawaii*, 138 S. Ct. 2392, 2416 (2018); *see also Clapper*, 568 U.S. at 411 ("[R]espondents fail to offer any evidence that their communications have been monitored under § 1881a, a failure that substantially undermines their standing theory."); *Halkin*, 690 F.2d at 999-1000 (holding that the absence of proof of actual acquisition of appellants' communications was fatal to their claims).

In *Clapper*, the Court found that allegations that plaintiffs' communications would be intercepted were too speculative, attenuated, and indirect to establish injury in fact that was fairly traceable to the governmental surveillance activities. 568 U.S. at 408-13. The *Clapper* Court held that plaintiffs lacked standing to challenge the NSA's surveillance under FISA because their "highly speculative fear" that they would be targeted by surveillance relied on a "speculative chain of possibilities" insufficient to establish a "certainly impending" injury. *Id.*

For their claim under the Wiretap Act, Plaintiffs must demonstrate an injury-in-fact occurred for each and every plaintiff where any communication traveling on the Internet backbone was intercepted, copied, or redirected, diverting it from its normal course. *See George v. Carusone*, 849 F. Supp. 159, 163 (D. Conn. 1994) (quoting *United States v. Rodriguez*, 968 F.2d 130, 136 (2d Cir. 1992), *cert. denied*, 506 U.S. 847 (1992)). For a claim under the Stored Communications Act, Plaintiffs must demonstrate an "injury from the collection, and maintenance in a government database, of records relating to them." *American Civil Liberties Union v. Clapper*, 785 F.3d 787, 801 (2d Cir. 2015); *see also Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 878 (9th Cir. 2002) (construing "intercept" in light of ordinary meaning, *i.e.*,, "to stop, or interrupt in progress or course before arrival.") (citation omitted).

///

///

C. Legal Standard on State Secrets Privilege.

The state secrets privilege has two applications: as a rule of evidentiary privilege, barring only the secret evidence from exposure during litigation, and as a rule of non-justiciability, when the subject matter of the lawsuit is itself a state secret, necessitating dismissal. *See Fazaga*, 916 F.3d at 1227; *see also American Civil Liberties Union v. National Security Agency*, 493 F.3d 644, 650 n.2 (6th Cir. 2007). The first application of evidentiary withholding can serve to remove only certain specific pieces of evidence or can be applied to compel the removal of a sufficiently broad swath of evidence which may have the consequence of requiring dismissal of the entire suit. Such a dismissal may be necessitated by the instances in which the removal of evidence disables a plaintiff from the ability to establish the *prima facie* elements of a claim without resort to privileged information or instances in which the removed evidence bars the defendant from establishing a defense. *See Kasza v. Browner*, 133 F.3d 1159, 1166 (9th Cir. 1998).

Once documents pursuant to a successful claim of privilege are withheld, the case may proceed with the omission of the secret or closely entangled evidence. Alternatively, if application of the state secrets bars too much, the court may be required to dismiss the action in its entirety. Such instances include when, without the secret evidence, a plaintiff is unable to prove the *prima facie* elements of a claim with nonprivileged evidence. *See id.* Or the privilege may apply to bar information that would otherwise give the defendant a valid defense to the claim, thus requiring dismissal. *See id.* Lastly, the court may be compelled to dismiss when, although the claims and defenses may be stated without reference to privileged evidence, "it may be impossible to proceed with the litigation because – privileged evidence being inseparable from nonprivileged information that will be necessary to the claims or defenses – litigating the case to a judgment on the merits would present an unacceptable risk of disclosing state secrets." *Mohamed v. Jeppesen Dataplan, Inc.*, 614 F.3d 1070, 1083 (9th Cir. 2009) (en banc) (citations omitted); *see also Farnsworth Cannon, Inc. v. Grimes*, 635 F.2d 268, 279-80 (4th Cir. 1980) (en banc) (per curiam) (Phillips, J., specially concurring and dissenting) (concluding that "litigation should be entirely foreclosed at the outset by dismissal of the

action" if it appears that "the danger of inadvertent compromise of the protected state secrets outweighs the public and private interests in attempting formally to resolve the dispute while honoring the privilege").

Alternatively, the state secrets privilege may be invoked to bar litigation of the matter in its entirety where "the trial of which would inevitably lead to the disclosure of matters which the law itself regards as confidential, and respecting which it will not allow the confidence to be violated." *Totten v. United States*, 92 U.S. 105, 107 (1875). Where the very subject matter of the lawsuit is a matter of state secret, the action must be dismissed without reaching the question of evidence. *See Al-Haramain Islamic Foundation, Inc. v. Bush*, 507 F.3d 1190, 1197 (9th Cir. 2007) ("*Al-Haramain*") (citations omitted); *see also Sterling v. Tenet*, 416 F.3d 338, 348 (4th Cir. 2005) (holding that dismissal is proper where "sensitive military secrets will be so central to the subject matter of the litigation that any attempt to proceed will threaten disclosure of the privileged matters.").

D. Analysis of Plaintiffs' Standing.

The Court finds that two of the required elements for standing are at issue at this procedural posture: the question whether any individual plaintiff suffered any concrete and particularized injury as well as the issue whether any potential injury could possibly be found to be redressable by a favorable judgment. The Court addresses both elements in order.

1. Plaintiffs' Evidentiary Proffer of Their Alleged Injury.

Throughout the pendency of this action, Plaintiffs have consistently argued that they have suffered injury by the creation of a large, untargeted, dragnet surveillance program designed to "intercept all or substantially all of its customers' communications, . . . [which] necessarily inflicts a concrete injury that affects each customer in a distinct way, depending on the content of that customer's communications and the time that customer spends using AT&T services." *Hepting v. AT&T Corp.*, 439 F. Supp. 2d 974, 1001 (N.D. Cal. 2006). In this matter, the Ninth Circuit has held that although the harm alleged by Plaintiffs is widely shared, that does not necessarily render it a generalized grievance. *See Jewel*, 673 F.3d at 909-10 ("[W]e

conclude that Jewel alleged a sufficiently concrete and particularized injury, Jewel's allegations are highly specific and lay out concrete harms arising from the warrantless searches.").

However, at the summary judgment stage where their allegations must be supported by specific facts, Plaintiffs continue to maintain that the NSA's surveillance programs must have been comprehensive to be effective. Plaintiffs assert that their allegations regarding whether their communications were intercepted in mass surveillance efforts are more likely than not true because of the large, untargeted nature of the program. Precisely this argument was rejected by the court in *Obama v. Klayman*, in which the court found that the assertions of standing based on mass comprehensive surveillance were too speculative and ultimately unpersuasive. 800 F.3d at 567 (holding that plaintiffs' "assertion that NSA's collection must be comprehensive in order for the program to be most effective is no stronger than the *Clapper* plaintiffs' assertions regarding the government's motive and capacity to target their communications."). In the absence of a factual predicate to establish any particular harm on behalf of any specific individual plaintiff, the Court must review and adjudicate the effect of the classified evidence regarding Plaintiffs' standing to sue. That review and adjudication is contained in the Court's Classified Order filed herewith.

In their attempt to establish the specific factual predicate based on public evidence for their contention that Plaintiffs have, as specific named individuals, been injured by interception of their communications, Plaintiffs rely in large part on the declarations of Mark Klein and James W. Russell and their proffered experts, as well as an additional former AT&T employee to present the relevant operational details of the surveillance program. Just as they had before when contesting the violation of their Fourth Amendment rights, Plaintiffs assert that these declarations support the contention that customers' communications were the subject of a dragnet seizure and search program, controlled by or at the direction of the Defendants. Having reviewed the factual record in its entirety, the Court finds the Plaintiffs' evidence does not support this claim.

Plaintiffs again rely on the declaration of Klein, a former AT&T technician who executed a declaration in 2006 about his observations involving the creation of a secure room at

the AT&T facility at Folsom Street in San Francisco. (Dkt. No. 84-2, Declaration of Mark Klein ("Klein Decl.") ¶¶ 8-18.) However, the Court confirms its earlier finding that Klein cannot establish the content, function, or purpose of the secure room at the AT&T site based on his own independent knowledge. *See* Fed. R. Civ. P. 56(c)(4). The limited knowledge that Klein does possess firsthand does not support Plaintiffs' contention about the actual operation of the data collection process or the alleged agency role of AT&T. Klein can only speculate about what data were actually processed and by whom in the secure room and how and for what purpose, as he was never involved in its operation. Lastly, the documents attached to Klein's declaration are not excepted from the hearsay objection on the basis that they are admissible business records. (Dkt. No. 84-3, 84-4, 84-5, 84-6, Klein Decl. Exs. A-C.) The timing of the creation of these attachments indicate that they were not simultaneous records of acts or events that were occurring at or around the time of the documents' creation. *See* Fed. R. Evid. 803(6).

Plaintiffs again propound the declaration of James Russell who relies on the Klein declaration and attached exhibits with regard to the interconnections between AT&T and other internet providers. (Dkt. No. 84-1, Declaration of James W. Russell ¶¶ 5, 6, 10, 12, 19-22.) Having twice found those exhibits inadmissible for the truth of the matters asserted therein, the Court similarly finds Russell's proffered conclusions unreliable.

To this existing evidentiary record, Plaintiffs now add the declaration of another former technician at AT&T, Phillip Long, who declares that without explanation, "sometime in the first half of the 2000s," he was directed to reroute AT&T's Internet backbone connections through the Folsom Street facility, "rather than through the nearest frame relay or ATM switch." (Dkt. No. 417-5, Declaration of Phillip Long ¶¶ 11, 12.) Long declares that he can offer no engineering or business reason for this reconfiguration. (*Id*. at ¶ 15.) The addition of Long's declaration does not serve to corroborate AT&T's participation in the alleged governmental collection program.

Plaintiffs' previously-disclosed experts, J. Scott Marcus and Dr. Brian Reid, rely upon Klein's observations and documents to formulate their expert opinions. Just as the Court determined in the context of the Fourth Amendment cross-motions for summary judgment with

regard to the Marcus opinion, the Court finds that these expert conclusions are not based on sufficient facts or data where the underlying declaration is based on hearsay and speculation. For example, Dr. Reid, relying upon the description of the Folsom facility furnished by Klein, offers an opinion about the likelihood that Plaintiffs' communications "passed through the peering site at AT&T's Facility . . . along with the rest of the traffic passing over all of the peering-link fibers into which splitters were installed . . . were replicated." (Dkt. No. 417-6, Declaration of Brian Reid ¶¶ 2, 20-23.) As the Court has found, the evidence relied upon by Plaintiffs' experts regarding the purpose and function of the secure equipment at AT&T and assumed operational details of the program is not probative as it is not based on sufficient facts or data. *See* Fed. R. Evid. 702(b).

In addition to these experts, Plaintiffs now proffer the opinions of two more experts, Ashkan Soltani and Matthew Blaze. Like the experts earlier proffered by Plaintiffs, Professor Blaze opines that, after review of the Klein declaration and exhibits, he believes "it is highly likely that the [internet] communications of all plaintiffs passed through peering-link fibers connected to the splitter . . . at the AT&T Folsom Street Facility." (Dkt. No. 417-7, Declaration of Matthew Blaze ¶¶ 2, 11, 41-46.) Again the Court has found that the evidence relied upon by Plaintiffs' expert regarding the purpose and function of the secure equipment at AT&T and assumed operational details of the program is not probative as it is not based on sufficient facts or data. *See* Fed. R. Evid. 702(b). Lastly, Plaintiffs proffer Mr. Soltani as an expert who opines that a surveillance network of the type Plaintiffs conjecture would also likely intercept the communications of users of cloud-based email applications such as Google's gmail or Yahoo mail. (Dkt. No. 417-8, Declaration of Ashkan Soltani ¶ 16.) This unquantified likelihood of interception regarding some users' email based on the posited Internet surveillance connection points and collection process is insufficient to constitute specific evidence of injury. Further, the premise upon which Mr. Soltani's opinion derives is not based on sufficient facts or data. *See* Fed. R. Evid. 702(b).

Plaintiffs further make the unsupported allegation that AT&T, Verizon, Verizon Wireless, and Sprint were acting in concert with or as agents of Defendants to produce phone

records in bulk.[1] Plaintiffs contend that the Government has admitted that these large service providers were participants in the NSA bulk collection of telephony metadata. In support of this contention, Plaintiffs submit a Primary Order issued by the Foreign Intelligence Surveillance Court ("FISC") authorizing the NSA to collect such bulk data for a 90-day period, from unidentified, redacted telecommunications service providers. (Dkt. No. 417-4, Declaration of Richard R. Weibe, Ex. A at 1.) This redacted order was issued in FISC docket Business Records ("BR") 10-10 and was declassified and publicly released by the Director of National Intelligence. (*Id.* at ¶ 3.) Plaintiffs also offer a copy of an excerpt from an NSA Inspector General compliance audit report which includes a letter regarding a non-compliance incident in the telephone call records program. (*See id.*, Ex. B at 28-29.) The excerpt of the report and attached letter were released in response to a Freedom of Information Act ("FOIA") lawsuit brought by the New York Times against the National Security Administration in 2015. (*See id.* at ¶ 4.) The letter, filed with the FISC, identifies in the caption the telecommunications companies, including AT&T, Verizon, Verizon Wireless, and Sprint, that were compelled by the Primary Order BR 10-10 to produce records. (*Id.*, Ex. B at 28.)

In response, Defendants contend that, although the redacted Primary Order from the FISC (in which the names of the providers were redacted) was authenticated by the Government, the second letter (which purports to identify the names of those providers) has not been authenticated by the Government.[2] Because the letter was inadvertently disclosed in an

---

[1] Plaintiffs have only been able to establish that the Government has admitted to working with Verizon Business Network Systems for a brief period of time, which does not indicate that data from other network providers were ever collected. *See Obama*, 800 F.3d at 563 (holding that because "plaintiffs are Verizon *Wirelesss* subscribers and not Verizon *Business Network Systems* subscribers . . . the facts marshaled by plaintiff do not fully establish that their own metadata was ever collected.").

[2] Defendants also argue that the letter has no evidentiary value as it was downloaded by Plaintiffs from the New York Times article written about the FOIA lawsuit. *See Schwarz v. Lassen County ex rel. Lassen County Jail*, 2013 WL 5425102, at *10 (E.D. Cal. Sept. 27, 2013) ("evidence procured off the Internet is adequate for almost nothing" without authentication). However, in response, Plaintiffs proffer the affidavit of an attorney for the New York Times in the FOIA lawsuit, who declares that the excerpt and attached letter were produced by the NSA in August 2015 in that matter. (*See* Dkt. No. 431, Declaration of David E. McGraw, ¶¶ 2, 5-6.) Mr. McGraw indicates that the attorneys representing the NSA at the Department of Justice notified him that the letter contained in the audit report had been "inadvertently produced" and had asked for its return. (*Id.* at ¶ 7.)

unrelated matter and has not been authenticated by the Government, the Court finds it cannot rely on it. *See, e.g., Al-Haramain*, 507 F.3d at 1205. Further, there has been no waiver of the state secret privilege over the document. The Court accepts Defendants' representation that whether or not the letter is authentic is itself classified information the disclosure of which could reasonably be expected to cause grave harm to national security. (*See also* Dkt. No. 422, Notice of Lodging of Classified Materials for *In Camera, Ex Parte* Review at 2, Declaration of Jonathan Darby, National Security Agency Director of Operations, ¶¶ 16-20.)

Lastly, Plaintiffs seek to introduce what is labeled a working draft of a report prepared by the Office of the Inspector General for the National Security Agency ("Draft OIG Report") with a supporting declaration from Edward Snowden. (Dkt. No. 432, Declaration of Edward J. Snowden, Ex. 1; Dkt. No. 147, Declaration of Richard R. Wiebe, Ex. A.) The Draft OIG Report does not in fact name AT&T or Verizon as participants in any possible collection efforts, it is labeled as a draft, and Defendants do not authenticate the exhibit. Accordingly, the Court finds it cannot rely on it. *See, e.g., Al-Haramain*, 507 F.3d at 1205. Plaintiffs' contention that Snowden may authenticate the purported NSA document is not persuasive, either by way of his current declaration or in the future through live testimony. *See Orr*, 285 F.3d at 773 (holding that a trial court may only consider admissible evidence on ruling on a motion for summary judgment and authentication is a "condition precedent to admissibility"). Further, there has been no waiver of the state secret privilege over the document and Defendants have objected on the basis of the privilege to Plaintiffs' requests for admissions regarding the authenticity of this document. (Dkt. No. 414-1, Government Defendants' Supplemental and Revised Response to Plaintiffs' Revised First Set of Requests for Admission Limited to Standing, at 70-73.)

The underlying premise that AT&T worked in the capacity of an agent for Defendants is without factual or substantive evidentiary support. And Plaintiffs have still not adduced admissible evidence of the actual equipment installed in the secure room or the activities conducted there. After review of the entirety of the evidentiary record, the Court finds the propounded evidence is not probative or admissible as to the actual conditions or purposes of the apparatus at the AT&T facility or their role at the time at issue in this case.

The Court finds that Plaintiffs have failed to proffer sufficient admissible evidence to indicate that records of their communications were among those affected by Defendants. Although there are materials in the public record that allude to possible surveillance programs, the Court finds that the "argument that 'the cat is already out of the bag' is unsupported by the record and contrary to the government's" classified submissions. *See Military Audit Project v. Casey*, 656 F.2d 724, 744-45 (D.C. Cir. 1981). Although in this public order, the Court is unable to address the sum of all evidence relevant to standing, the Court has addressed the classified evidence relating to standing in detail in its Classified Order, filed in conjunction with this one. (*See* Classified Order Section I.) Although neither the Court nor Defendants can confirm or deny the allegations as made by Plaintiffs in their proffer of evidence in support of standing, the Court addresses the operative, but classified, facts separately in detail.

In addition, having reviewed the classified portion of the record, the Court concludes that even if the public evidence proffered by Plaintiffs were sufficiently probative to establish standing, adjudication of the standing issue could not proceed without risking exceptionally grave damage to national security. The details of the alleged data collection process that are subject to the Defendants' assertion of the state secrets privilege are necessary to address Plaintiffs' theory of standing as well as to engage in a full and fair adjudication of Defendants' substantive defenses.

2. Redressability.

Another necessary element to establish Article III standing is the requirement that any concrete and particularized injury be "redressable by a favorable ruling.'" *Clapper*, 568 U.S. at 409. Here, the Court cannot issue a judgment without exposing classified information. And, by evaluating the classified information, the Court has determined that it cannot render a judgment either as to the merits or as to any defense on the issue of standing. Any finding or final judgment would disclose information that might imperil the national security. *See, e.g., Klayman*, 800 F.3d at 568 (finding that "the government's silence regarding the scope of bulk collection is a feature of the program, not a bug.") (citing *Clapper*, 568 U.S. at 412 n.4 ("the court's postdisclosure decision about whether to dismiss the suit for lack of standing would

surely signal to the terrorist whether his name was on the list of surveillance targets.")). The same "considerations apply with equal force here, where the government has sought to maintain a similarly strategic silence regarding the scope of its bulk collection." *Id.* In order to issue a dispositive decision on the standing issue, a finding of standing would necessitate disclosure of possible interception of plaintiffs' communications, thereby signaling injury. Such a disclosure may imperil national security. Any attempt to prove the specific facts of the programs at issue, or to defend against the Plaintiffs' analysis of the programs would risk disclosure of the locations, sources, methods, assisting providers, and other operational details of Defendants' intelligence-gathering activities. At this advanced procedural posture, the Court is bound to accept the Defendants' representation that disclosure of these details reasonably could be expected to cause exceptionally grave damage to national security.

Even if, utilizing only public evidence, the Plaintiffs could ostensibly plead sufficient facts to support their claim of standing to pursue their remaining statutory causes of action, the Court finds that it faces the intractable problem that proceeding further with this case would cause exceptionally grave harm to the national security. The Court cannot issue any determinative finding on the issue of whether or not Plaintiffs have standing without taking the risk that such a ruling may result in potentially devastating national security consequences. *See, e.g., Clapper*, 568 U.S. at 412 n.4. Notwithstanding the fact that this Court has thoroughly reviewed all of the evidence submitted with regard to Plaintiffs' standing, making any determination to address Plaintiffs' allegations regarding the scope of the data collection program would risk informing adversaries of the specific nature and operational details of the process and scope of Defendants' participation in the program. Accordingly, the Court finds that Plaintiffs are unable to show either that they have suffered a concrete and particularized injury or that any such potential injury could be redressable by a favorable ruling. As the Ninth Circuit predicted early on in the development of this case, "procedural, evidentiary, and substantive barriers" might ultimately doom Plaintiffs' proof of standing. *Jewel*, 673 F.3d at 911. This Court found, and the Ninth Circuit has affirmed, that the assertion of the state secrets privilege did not warrant dismissal at the pleadings stage without a thorough and complete

investigation of the evidence. *Jewel*, 965 F. Supp. 2d 1090, 1105-06 (N.D. Cal. 2013); *Jewel*, 673 F.3d at 909-10; *see also Fazaga*, 916 F.3d at 1226, 1232, 1234. However, the Court, after extensive *in camera* review of the classified materials and a similarly thorough review of the public evidence, finds that making any particularized determination on standing in order to continue with this litigation may imperil the national security.[3] The Court also addresses this finding in its Classified Order.

E. Defendants' Assertion of the State Secrets Privilege.

The privilege asserted by Defendants here seeks to protect information vital to the national security and may be invoked by the Government where it is shown, "from all the circumstances of the case, that there is a reasonable danger that compulsion of the evidence will expose . . . matters which, in the interest of national security, should not be divulged." *United States v. Reynolds*, 345 U.S. 1, 6-7 (1953).

The analysis of whether the state secrets privilege applies involves three distinct steps. First, the Court must ascertain whether the procedural requirements for invoking the privilege have been satisfied. *Jeppesen*, 614 F.3d at 1080 (quoting *Al-Haramain*, 507 F.3d at 1202). Second, the Court must make an independent determination whether the information is privileged. In determining whether the privilege attaches, the Court may consider a party's need for access to the allegedly privileged materials. *See Reynolds*, 345 U.S. at 11. Lastly, the "ultimate question to be resolved is how the matter should proceed in light of the successful privilege claim." *El-Masri v. United States*, 479 F.3d 296, 304 (4th Cir. 2007).

In order to satisfy the requirements of the first step, the Government must submit a "formal claim of privilege, lodged by the head of the department which has control over the matter, after actual personal consideration by that officer." *Id.* (quoting *Reynolds*, 345 U.S. at 7-8). The assertion of privilege "must by presented in sufficient detail for the court to make an

[3] After thorough review of the evidence submitted in relation to Plaintiffs' statutory claims and marshaled by Defendants to satisfy the Court's broader order regarding the threshold standing issue, the Court is satisfied that its analysis of the Fourth Amendment standing to sue remains law of the case and rests on solid legal ground. *See Jewel v. National Security Agency*, 2015 WL 545925, at *5 (N.D. Cal. Feb. 10, 2015). Therefore, Plaintiffs' request to reconsider that decision is DENIED.

independent determination of the validity of the claim of privilege and the scope of the evidence subject to the privilege." *Id.* Such an invocation must be made only after "serious, considered judgment, not simply [as] an administrative formality." *United States v. W.R. Grace*, 526 F.3d 499, 507-08 (9th Cir. 2008) (en banc). "The formal claim must reflect the certifying official's personal judgment . . . [and] must be presented in sufficient detail for the court to make an independent determination of the validity of the claim of privilege and the scope of the evidence subject to the privilege." *Jeppesen*, 614 F.3d at 1080.

The Court finds that this step has been satisfied by the submission of the public declaration of the Principal Deputy Director of National Intelligence, serving as Acting Director of National Intelligence and acting head of the Intelligence Community, following her personal consideration of the matters at issue here. (*See* Dkt. No. 388-2, Declaration of Principal Deputy Director of National Intelligence, ¶¶ 8, 19; Dkt. No. 104, Declaration of James R. Clapper ¶ 2; Dkt. No. 168, Declaration of James R. Clapper ¶ 2.) This claim of privilege is further supported by the declaration of Admiral Michael Rogers, in which he explains the nature of the evidence itself and details the specific harms that could be expected to result from disclosure of the information. (*See* Dkt. No. 389, Rogers Decl. ¶¶ 2, 331; *see also* Classified Order at n.1.)

In order to satisfy the requirements of the second step, the Court is able to assess independently, based on both the public and classified submissions by Defendants, and from all of the evidence in the record accumulated over the years of litigating this case, that there is a reasonable danger the disclosure of the information at issue here would be harmful to national security. *See, e.g., Jewel*, 965 F. Supp. 2d at 1103; *Jewel*, 2015 WL 545925, at *1, *5. The Court must "sustain a claim of privilege when it is satisfied, 'from all the circumstances of the case, that there is a reasonable danger that compulsion of the evidence will expose . . . matters which, in the interest of national security, should not be divulged.'" *Jeppesen*, 614 F.3d at 1081 (quoting *Reynolds*, 345 U.S. at 10). Here, the Court has made "an independent determination whether the information is privileged." *Al-Haramain*, 507 F.3d at 1202. In making this determination, the Court must strike the appropriate balance "between protecting national security matters and preserving an open court system." *Id.* at 1203. "This inquiry is a difficult

one, for it pits the judiciary's search for truth against the Executive's duty to maintain the nation's security." *El-Masri*, 479 F.3d at 304. In evaluating the need for secrecy, the Court must defer to the Executive on matters of foreign policy and national security. *See Jeppesen*, 614 F.3d at 1081-82. However, the assertion of the state secrets doctrine does not "represent a complete surrender of judicial control over access to the courts." *El-Masri*, 479 F.3d at 312. Rather, in order to ensure that the doctrine is not asserted more frequently and sweepingly than necessary, "it is essential that the courts continue critically to examine instances of its invocation." *Ellsberg v. Mitchell*, 709 F.2d 51, 58 (D.C. Cir. 1983). However, should the Court find that the materials must not be divulged, "the evidence is absolutely privileged, irrespective of the plaintiffs' countervailing need for it." *See Jeppesen*, 614 F.3d at 1081 (citing *Reynolds*, 345 U.S. at 11).

The final element of the determination regarding the Government's assertion of the state secrets privilege is the court answering the ultimate question regarding how the matter should proceed in light of the legitimate claim of privilege. *See Jeppesen*, 614 F.3d at 1080. "The court must assess whether it is feasible for the litigation to proceed without the protected evidence and, if so, how." *Id.* at 1082. When the Government successfully invokes the state secrets privilege, "the evidence is completely removed from the case." *Kasza*, 133 F.3d at 1166. The court is then tasked with disentangling the nonsensitive information from the privileged evidence. Often, after the privileged evidence is excluded, "the case will proceed accordingly, with no consequences save those resulting from the loss of evidence." *Al-Haramain*, 507 F.3d at 1204 (quoting *Ellsberg*, 709 F.3d at 64). However, there "will be occasions when, as a practical matter, secret and nonsecret information cannot be separated. In some cases, therefore, 'it is appropriate that the courts restrict the parties' access not only to evidence which itself risks the disclosure of a state secret, but also those pieces of evidence or areas of questioning which press so closely upon highly sensitive material that they create a high risk of inadvertent or indirect disclosures.'" *Jeppesen*, 614 F.3d at 1082 (quoting *Bareford v. Gen. Dynamics Corp.*, 973 F.2d 1138, 1143-44 (5th Cir. 1992)); *see also Kasza*, 133 F.3d at 1166 ("[I]f seemingly innocuous information is part of a . . . mosaic, the state secrets privilege

may be invoked to bar its disclosure and the court cannot order the government to disentangle this information from other [*i.e.*, secret] information.")

Plaintiffs maintain that the Ninth Circuit's recent decision in *Fazaga* precludes the Court from dismissing this case on state secrets grounds, and that the Court must use the procedures of Section 1806(f) to decide Plaintiffs' statutory claims notwithstanding Defendants' assertions that even a finding on the threshold question of standing will cause grave harm to national security. *Fazaga* addressed a challenge to an allegedly unlawful FBI counter-terrorism investigation involving electronic surveillance. 916 F.3d at 1210-11. The district court dismissed all but one of plaintiff's claims at the pleading stage without further discovery based on the Government's assertion of the state secrets privilege. *Id.* at 1211. The Ninth Circuit reversed, concluding that Section 1806(f)'s procedures are to be used when "aggrieved persons" challenge the legality of electronic surveillance and that the district court erred by dismissing the case without reviewing the evidence, "including the evidence over which the Attorney General asserted the state secrets privilege, to determine whether the electronic surveillance was lawfully authorized and conducted." *Id.* at 1238, 1252.

Defendants contend that the *ex parte*, *in camera* procedures authorized under Section 1806(f) apply only to the determination of whether alleged electronic surveillance was lawful, and not to the threshold determination of whether Plaintiffs are "aggrieved persons" who have been subject to surveillance in the first place. *See, e.g.*, *Wikimedia Foundation v. National Security Agency*, 335 F. Supp. 3d 772, 786 (D. Md. 2018). In other words, in Defendants' view, Section 1806(f) displaces the state secrets privilege only as to a determination of lawfulness *after* Plaintiffs' standing has been demonstrated using non-classified evidence. The Court notes that in the procedural posture in which *Fazaga* reached the Ninth Circuit, the plaintiff's status as an aggrieved person had not yet been tested through discovery. Thus, the Ninth Circuit was not presented with the issue of what to do when, as here, the answer to the question of whether a particular plaintiff was subjected to surveillance – *i.e.*, is an "aggrieved person" under Section 1806(f) – is the very information over which the Government seeks to assert the state secrets privilege. Instead, in remanding for further proceedings, the court in *Fazaga* held that "[t]he

complaint's allegations are sufficient *if proven* to establish that Plaintiffs are 'aggrieved persons.'" *Id.* at 1216 (emphasis added).

This Court owes significant deference to the Executive's determination that, as described at oral argument, even a simple "yea or nay" as to whether Plaintiffs have standing to proceed on their statutory claims would do grave harm to national security. *See Jeppesen*, 614 F.3d at 1081-82 ("In evaluating the need for secrecy, 'we 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.'") (quoting *Al-Haramain*, 507 F.3d at 1203); *see also Al-Haramain*, 507 F.3d at 1203 ("[A]t some level, the question whether Al-Haramain has been subject to NSA surveillance may seem, without more, somewhat innocuous . . . . But our judicial intuition about this proposition is no substitute for documented risks and threats posed by the potential disclosure of national security information."). The Court has not "accept[ed] at face value the government's claim or justification of privilege" on the issue of Plaintiffs' standing to pursue their remaining statutory claims, but instead has reviewed all of the classified evidence submitted by Defendants in response to Plaintiffs' discovery requests and this Court's orders. *See id.* That comprehensive review distinguishes this case from *Fazaga*, and in fact from any other case involving state secrets cited by the parties or known to this Court. Under the unique procedural posture of this case, and where the very issue of standing implicates state secrets, the Court finds that it is not foreclosed under the holding in *Fazaga* and Section 1806(f) from now dismissing on state secrets grounds.

Here, having reviewed the materials submitted and having considered the claims alleged and the record as a whole, the Court finds that, just as they did when disputing the violation of the Fourth Amendment in the parties' previous cross-motions for summary judgment, Defendants have again successfully invoked the state secrets privilege. This Court has previously found and maintains that, given the multiple public disclosures of information regarding the surveillance program, the very subject matter of the suit does not constitute a state secret. However, at this procedural posture and with the development of a full and extensive

record on the threshold issue of standing, the Court finds that permitting further proceedings would jeopardize the national security.

The Court finds that because a fair and full adjudication of the Plaintiffs' claims and the Defendants' defenses would require potentially harmful disclosures of national security information that are protected by the state secrets privilege, the Court must exclude such evidence from the case. *See Jeppesen*, 614 F.3d at 1083 (holding that "application of the privilege may require dismissal" of a claim if, for example, "the privilege deprives the plaintiff of information needed to set forth a prima facie case, or the defendant of information that would otherwise give the defendant a valid defense to the claim"). Addressing any defenses involves a significant risk of potentially harmful effects any disclosures could have on national security. *See Kasza*, 133 F.3d at 1166.

Having allowed the full development of the record and having reviewed the universe of documents and declarations produced by both parties to this action both publicly and under the procedures of Section 1806(f) of FISA, the Court finds that it has reached the threshold at which it can go no further. The Court accepts the assertion of the state secrets privilege at this procedural juncture to mandate the dismissal of this action. Accordingly, based on both the determination that it cannot rule whether or not Plaintiffs have standing to proceed and that the well-founded assertion of privilege mandates dismissal, the Court GRANTS Defendants' motion for summary judgment and DENIES Plaintiffs' cross-motion to proceed to resolution on the merits.[4]

F. Plaintiffs' Request for Additional Discovery and for Discovery Sanctions.

Further, having reviewed the universe of classified and public documents produced by Defendants, the Court is satisfied that Defendants have met their discovery obligations. (*See* Classified Order at 2.) The Court finds that no evidentiary sanction for evidence spoliation

[4] As to all remaining claims, judgment is entered against Government officials in their personal capacities for both damages and equitable relief under the Constitutional and statutory provisions. The personal-capacity claims were stayed pending "resolution of any dispositive motion by the Government Defendants." (Order granting stipulation, Dkt. No. 93 at 1-2.) Having granted summary judgment in favor of Defendants, all personal-capacity claims are resolved in Defendants' favor as well.

is warranted and there is no basis to grant Plaintiffs' request to continue the resolution of the cross-motions for summary judgment pursuant to Federal Rule of Civil Procedure 56(d). In light of the Court's determination that this action cannot proceed further, under Section 1806(f) or otherwise, disclosure to the Plaintiffs of the classified evidence submitted by Defendants is not "necessary to make an accurate determination of the legality of the surveillance." 50 U.S.C. § 1806(f). Accordingly, Plaintiffs' renewed requests for access to the classified evidence Defendants have submitted, for a further declassification review of that evidence, and for further discovery or evidentiary sanctions are DENIED.

CONCLUSION

For the foregoing reasons, the Court GRANTS Defendants' motion for summary judgment and DENIES Plaintiffs' cross-motion for summary judgment. The Court shall issue a separate classified order which shall be preserved in the Court's sealed record pending any further proceeding. All classified evidence lodged with the Court by Defendants shall also be so preserved in the sealed record. A separate judgment will issue and the Clerk shall close the file.

IT IS SO ORDERED.

Dated: April 25, 2019

JEFFREY S. WHITE
UNITED STATES DISTRICT JUDGE

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

CAROLYN JEWEL, ET AL.,

Plaintiffs,

v.

NATIONAL SECURITY AGENCY, ET AL.,

Defendants.

/

No. C 08-04373 JSW

ORDER REGARDING DISCOVERY DISPUTE

The Court has reviewed the parties' discovery dispute submitted on August 24, 2018. Plaintiffs contend that the Government has circumvented the federal rules governing discovery by failing to provide separate and individual responses to each of Plaintiffs' Requests for Admission.

The Court has diligently reviewed the materials submitted in response to all of Plaintiffs' discovery requests. In addition to the delineated objections in the public record and the redacted versions of the Government's declarations, the form of the Government's classified responses satisfies the Court's instructions. Although the Government's substantive responses to the Requests for Admission are organized thematically and by category, the Court finds that, in this unique procedural posture, the Government has fully and fairly complied with the Court's instructions to marshal the evidence relevant to the standing issue.

Accordingly, Plaintiffs' request for an order to require the Government to respond separately and individually to each of Plaintiffs' Requests for Admission is DENIED and the briefing schedule on dispositive motions remains as currently set.

IT IS SO ORDERED.

Dated: August 28, 2018

JEFFREY S. WHITE
UNITED STATES DISTRICT JUDGE

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

CAROLYN JEWEL, ET AL.,

Plaintiffs,

v.

NATIONAL SECURITY AGENCY, ET AL.,

Defendants.

/

No. C 08-04373 JSW

ORDER REQUIRING DISPOSITIVE MOTIONS BRIEFING

The Court has reviewed the classified materials provided by the Government Defendants and the parties' most recent briefs in response to the Court's questions. Mindful of the appellate court's admonition to address the parties' substantive claims in a comprehensive and expeditious fashion, the Court HEREBY ORDERS the parties file dispositive motions to resolve the threshold legal issues raised by the remaining statutory claims in this matter.

The Government Defendants shall address why, assuming for the sake of argument only that the classified evidence could demonstrate that Plaintiffs have suffered an injury in fact as to their remaining statutory claims, the state secrets privilege nevertheless applies in this case and requires dismissal.

In this matter, when addressing whether the state secrets doctrine effectively served to bar this litigation as a matter of law at the initial pleading stage, the Court found that it was tasked with the review and examination of classified documents under the procedural

mechanism prescribed under the Foreign Intelligence Surveillance Act ("FISA"), 50 U.S.C. § 1806(f). *Jewel v. National Security Agency*, 965 F. Supp. 2d 1090, 1103 (N.D. Cal. July 23, 2013). After requiring the production of documents responsive to the Plaintiffs' discovery requests relevant to the predicate issue of standing and having now reviewed the classified materials regarding Plaintiffs' assertion of standing *in camera* and *ex parte* under the procedural mechanism provided by FISA, the Court is now tasked with the broader substantive question of whether "even if the claims and defenses might theoretically be established without relying on privileged evidence, it may be impossible to proceed with the litigation because . . . litigating the case to a judgment on the merits would present an unacceptable risk of disclosing state secrets." *Mohamed v. Jeppesen Dataplan, Inc.*, 614 F.3d 1070, 1083 (9th Cir. 2010) (en banc). Plaintiffs' position that once the procedures for the handling of materials and information set forth in section 1806(f) have been invoked, the state secrets doctrine may not be a potential substantive bar to the ongoing litigation is inaccurate. *Cf. In re National Security Agency Telecommunications Records Litigation*, 564 F. Supp. 2d 1109, 1119 (N.D. Cal. July 2, 2008) (differentiating the applicable "process[es]," "procedure[s]," and "protocol[s]" under section 1806(f) and under the state secrets privilege).

Plaintiffs shall address, using only available public evidence, whether they can meet their burden to establish that they have standing as to each of their remaining statutory claims. In their response, the Government Defendants shall substantively address the factual evidence relating to Plaintiffs' standing or lack thereof relying on both the public and classified materials submitted (any reference made to classified materials may be filed as a separate classified submission).

The Government Defendants shall file an opening brief not to exceed 25 pages by no later than September 7, 2018. Plaintiffs shall file a brief in opposition and cross-motion not to exceed 25 pages by no later than September 28, 2018. The Government Defendants shall file their reply and opposition to the cross-motion not to exceed 25 pages by no later than October 12, 2018. Plaintiffs shall file their reply in support of the cross-motion not to exceed 15 pages by no later than October 26, 2018.

The Court is also aware of the various delays and complex procedural course this case has taken as well as the Ninth Circuit's mandate comprehensively and expeditiously to address the threshold legal issues in this matter. Without a persuasive showing of good cause, there will be no extensions of this briefing schedule. Plaintiffs' contentions about the Government Defendants' alleged spoliation of evidence or sufficiency of their discovery responses are not adequate bases for an extension of time.

The Court shall set a hearing on the cross-motions by separate order, if necessary.

IT IS SO ORDERED.

Dated: August 17, 2018

JEFFREY S. WHITE
UNITED STATES DISTRICT JUDGE

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

CAROLYN JEWEL, ET AL.,

Plaintiffs,

v.

NATIONAL SECURITY AGENCY, ET AL.,

Defendants.

/

No. C 08-04373 JSW

ORDER DENYING PLAINTIFFS' MOTION FOR ACCESS TO CLASSIFIED DISCOVERY MATERIALS AND REQUIRING ADDITIONAL BRIEFING

At the case management conference held in this matter on May 19, 2017, the Court ordered the Government Defendants to marshal all of their evidence relating to Plaintiffs' standing and to present that evidence to the Court, making as much of it public as possible. The Court directed the Government to file its unclassified responses to Plaintiff's revised discovery requests on the public record and to submit classified materials responsive to Plaintiffs' requests *ex parte* and *in camera*.

On April 1, 2018, Defendants' production was complete. On May 7, 2018, Plaintiffs filed a motion to obtain access to the classified materials pursuant to 18 U.S.C. Section 2712(b)(4). The Government Defendants oppose Plaintiffs' request. The Court, having considered the parties' respective submissions, DENIES Plaintiffs' motion for access. The Court is tasked with review of the materials *ex parte* and *in camera* and shall conduct such a review. The hearing set for July 6, 2018 is HEREBY VACATED.

In aid of making a proper assessment of the materials submitted by the Government Defendants, however, the Court HEREBY ISSUES the following order to the parties. The parties shall submit simultaneous briefing not to exceed 20 pages by no later than July 6, 2018,

on the current state of law on the following issues to aid the Court's *ex parte* and *in camera* review:

(1) whether the disclosure of the classified materials could be reasonably expected to cause harm to national security;

(2) whether the scope of the classified materials, provided it indeed does disclose "a voluminous amount of exceptionally detailed information about sources, methods, and operations of six separate NSA surveillance programs conducted over a period of nearly 20 years" requires that the Court uphold the Government's assertions of privilege, and mandate removing the evidence from the case entirely; what effect this action would have on the remainder of the case;

(3) in what circumstances could Plaintiffs proceed on the merits of their claims without access to the evidence establishing whether or not they have standing to sue;

(4) are there any examples of similar cases where classified or confidential information is withdrawn from the case but the presumption of standing is asserted; how can Plaintiffs establish they may be aggrieved persons without access to the information;

(5) setting aside the issue of the classified nature of the documents at issue, address the current legal standard for asserting standing in these circumstances.

IT IS SO ORDERED.

Dated: June 13, 2018

JEFFREY S. WHITE
UNITED STATES DISTRICT JUDGE

United States District Court
For the Northern District of California

UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

CIVIL MINUTE ORDER

DATE: May 19, 2017 Time in Court: 1 hour 54 minutes

JUDGE: JEFFREY S. WHITE Court Reporter: Diane Skillman

Courtroom Deputy: Jennifer Ottolini

CASE NO. C-08-4373 JSW
TITLE: Carolyn Jewel, et al., v. National Security Agency, et al.,

COUNSEL FOR PLAINTIFF:
Richard Wiebe
Cindy Cohn
Philip Tassin
Thomas Moore

COUNSEL FOR DEFENDANT:
James Gilligan
Rodney Patton
Caroline Anderson

PROCEEDINGS: Further Case Management Conference

RESULTS: Further Case Management Conference held.

By 6-2-17: Government counsel to inform the Court if, hypothetically, a career law clerk was granted security clearance, would she be able to view all documents, including those already produced in classified submissions.

The Court set the following schedule re Staged Discovery:

- 6-19-17: Plaintiffs to serve narrowed discovery requests on standing.
- 7-10-17: Parties shall meet and confer to agree to further limit requests based on Rule 26 with an eye toward significantly narrowing requests.
- 8-9-17: Defendants' responses due (presumably in public record). All questions need some sort of response - including whether some responses would be classified.

The remainder of discovery responses in dispute to be submitted ex parte and in camera, including but not limited to orally ordered scope of production on Defendants to marshal all evidence pertaining to statutory discovery issues.

Briefing and hearing on omnibus motions shall be set in the Order on Discovery.

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

CAROLYN JEWEL, ET AL.,

Plaintiffs,

v.

NATIONAL SECURITY AGENCY, ET AL.,

Defendants.
_____/

No. C 08-04373 JSW

ORDER GRANTING JOINT REQUEST FOR CASE MANAGEMENT CONFERENCE

Now before the Court is the parties' joint request for a case management conference. The request is GRANTED and shall be set on May 19, 2017 at 11:00 a.m. A joint case management conference statement shall be filed no later than May 5, 2017 in order to allow the Court sufficient time to review it and perhaps issue further questions. The discovery dispute with respect to Plaintiffs' remaining statutory claims under the Wiretap Act and Stored Communications Act brought against defendants National Security Agency, United States and the Department of Justice ("Defendants") under Counts 9, 12, and 15 of the complaint is pending and shall be addressed at the case management conference.

In response to the Ninth Circuit's earlier directive on initial remand to determine whether the government's assertion that the state secrets privilege barred the suit altogether, this Court resolved that the procedural mechanism under 50 U.S.C. section 1806(f) of the Foreign Intelligence Surveillance Act ("FISA") displaces the state secrets privilege. (Order dated July

23, 2013.) Defendants moved to dismiss all of Plaintiffs' claims, asserting that sovereign immunity barred litigation of Plaintiffs' statutory claims, and that the state secrets privilege required dismissal of the case in its entirety because attempting to litigate this matter to a judgment on the merits would present an unacceptable risk of disclosing state secrets. Plaintiffs cross-moved for partial summary judgment on the ground that the state secrets privilege is preempted by the procedure described in FISA section 106, 50 U.S.C. section 1806(f). In its order, the Court determined that with respect to Plaintiffs' statutory claims under the Wiretap Act, 18 U.S.C. section 2511(1), and the Electronic Communications Privacy Act or Stored Communications Act, 18 U.S.C. section 2703, that 18 U.S.C. section 2712 waives sovereign immunity for damages claims. (*Id.* at 15-18.) The Court also specifically found that section 2712(b)(4) "designat[es] Section 1806(f) as 'the exclusive means by which materials [designated as sensitive by the government] shall be reviewed' in suits against the United States under FISA, the Wiretap Action, and the Electronic Privacy Protection Act." (Order dated July 23. 2013 at 13.)[1]

The current state of the pleadings requires that the Court allow Plaintiffs to pursue their statutory claims for damages. The Ninth Circuit has explicitly cautioned this Court not to dispose of the issue of standing at the pleading stage. *See Jewel v. National Security Agency*, 673 F.3d 902, 911 (9th Cir. 2011). Although "[u]ltimately Jewel may face . . . procedural, evidentiary and substantive barriers . . . , at this initial pleading stage, the allegations are deemed true and are presumed to 'embrace the 'specific facts' needed to sustain the complaint.'" *Id.* (citing *Lujan v. Nat'l Wildlife Fed.*, 497 U.S. 871, 888 (1990)). Particularly, in the area of their statutory claims, this Court has found that in the absence of sovereign immunity, Plaintiffs may state claims under the Wiretap Act and the Stored Communications Act. The Ninth Circuit has found in this matter that "Congress specifically envisioned plaintiffs challenging government surveillance under this statutory constellation." *Id.* at 913. As to

[1] The Court queries the parties about the status of Plaintiffs' claims for violation of the First Amendment (counts 3 and 4) as well as their claim for violation of the separation of powers (count 17). The parties should address Plaintiffs' ability to pursue discovery on those claims as the parties agree that the same procedural mechanism, to the extent it applies at all, would apply to those claims just as it would to the statutory claims.

Jewel's statutory claims, "injury required by Article III may exist solely by virtue of statutes creating legal rights, the invasion of which creates standing." *Id.* at 908 (citing *Lujan v. Nat'l Wildlife Fed.*, 504 U.S. 555, 578 (1992)).[2]

Even considering the interim flux in relevant precedent and transitions in law, the Court has not received a dispositive motion to adjudicate Plaintiffs' remaining claims. The Court is similarly aware of the Ninth Circuit's specific directive to advance the conclusion of this litigation. Accordingly, the remaining statutory claims must be litigated and are currently ripe for discovery. The procedural mechanism under 50 U.S.C. section 1806(f) of FISA may serve to alleviate the risk of disclosure of state secret information.

In their joint submission to be filed no later than May 5, 2017, the parties shall address all of the topics set forth in the Standing Order for All Judges of the Northen District of California - *Contents of Joint Case Management Statement*, which can be found on the Court's website located at http://www.cand.uscourts.gov. *See* N.D. Civ L.R. 16-9 and 16-10(d).

In addition to these requirements, the parties shall meet and confer to address the following specific questions in an effort to arrive a joint proposal:

1. Defendants contend that *any* discovery of the NSA's programs is absolutely protected from disclosure by section 6 of the National Security Agency Act, 50 U.S.C. § 3605. If so, can Defendants move for judgment on the pleadings or otherwise position this matter for comprehensive resolution of the matter on the merits? By what mechanism can the Court address Defendants' central contention that the potential risk to national security may still be too great to pursue confirmation of the facts relating to the scope of the alleged governmental programs?

2. If this matter cannot be resolved as a matter of law and brought to the Ninth Circuit as a comprehensive appeal, the litigation of the remaining claims and the task of discovery must proceed. However, with regard to the submitted

[2] In this regard, the Court questions whether the holding in *Spokeo, Inc. v. Robins*, --- U.S. ---, 136 S. Ct. 1540, 1547 (2016), potentially alters the landscape regarding the Ninth Circuit's standing analysis in this matter.

discovery dispute, Plaintiffs have served 190 request for admissions, with multiple subparts and 70 interrogatories. This expansive and compound use of discovery is improper. Plaintiffs must be tasked with limiting their discovery to seek relevant documents and information pertaining to elements of the remaining claims. In what way do Plaintiffs propose to reasonably limit their discovery requests?

3. Have the parties considered staging discovery and perhaps beginning with discovery designed to establish standing? Can the Court determine the question of Plaintiffs' standing without reliance on classified materials? Are any of the classified materials already submitted responsive to the question of standing or responsive to Plaintiffs' current discovery requests? As the parties move past the pleadings phase and pursue discovery, how can Plaintiffs avoid the problem raised by *Clapper v. Amnesty International, USA*, 133 S Ct. 1138, 1148 n.4 (2013), regarding their burden to demonstrate that they are individually aggrieved persons, even in the mass surveillance context?

4. Can a Magistrate Judge with sufficient clearance help to aid the parties in narrowing their discovery requests and fashioning appropriate responses? Can the Court appoint a Special Master with sufficient clearance to aid the parties?

5. Once the discovery requests are sufficiently narrowed, can Defendants identify responsive documents, perhaps produce a log of the types of documents to Plaintiffs, and argue about whether they are discoverable in camera and *ex parte*?

6. Will the parties agree to allow career law clerk(s) who have security clearance to review classified documents already submitted in this matter or any further documents that may be produced in camera?

7. Can the parties submit a joint schedule in accordance with Federal Rule of Civil Procedure 16(b) to advance the timely and final resolution of this matter?

At the case management conference, the parties shall be prepared to answer any and all further questions posed by the Court regarding the best way to proceed to insure the timely progress of this litigation.

IT IS SO ORDERED.

Dated: March 21, 2017

JEFFREY S. WHITE
UNITED STATES DISTRICT JUDGE

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

CAROLYN JEWEL, ET AL.,

Plaintiffs,

v.

NATIONAL SECURITY AGENCY, ET AL.,

Defendants.

No. C 08-04373 JSW

VIRGINIA SHUBERT, ET AL.,

Plaintiffs,

v.

BARACK OBAMA, ET AL.,

Defendants.

No. C 07-00693 JSW

ORDER GRANTING MOTION TO LIFT STAY OF DISCOVERY

/

Now before the Court is Plaintiffs' motion to lift the Court's stay of discovery with respect to Plaintiffs' statutory claims under the Wiretap Act and Stored Communications Act brought against defendants National Security Agency, United States and the Department of Justice under Counts 9, 12, and 15 of the complaint. The Court finds the motion suitable for disposition without oral argument. *See* N.D. Civ. L.R. 7-1(b). Accordingly, the Court VACATES the hearing scheduled for February 26, 2016. Having considered the parties'

papers, relevant legal authority, and the record in this case, the Court GRANTS Plaintiffs' motion to lift the Court's stay of discovery.

In order to manage this matter in a manner most conducive to the unique concerns and challenges this case presents, the Court had stayed discovery pending resolution of challenged issues of law. However, having resolved the issue whether the Plaintiffs have sufficiently stated allegations to support claims for damages under the Wiretap Act and the Stored Communications Act, and having received explicit admonition from the Ninth Circuit Court of Appeals to advance this matter, the Court GRANTS Plaintiffs' motion to lift the stay of discovery with respect to Counts 9, 12, and 15.

In response to the Ninth Circuit's earlier directive on initial remand to determine whether the government's assertion that the state secrets privilege barred the suit altogether, this Court resolved that the procedural mechanism under 50 U.S.C. section 1806(f) of the Foreign Intelligence Surveillance Act ("FISA") displaces the state secrets privilege. (Order dated July 23, 2013.) Defendants moved to dismiss all of Plaintiffs' claims, asserting that sovereign immunity barred litigation of Plaintiffs' statutory claims, and that the state secrets privilege required dismissal of the case in its entirety because attempting to litigate this matter to a judgment on the merits would present an unacceptable risk of disclosing state secrets. Plaintiffs cross-moved for partial summary judgment on the ground that the state secrets privilege is preempted by the procedure described in FISA section 106, 50 U.S.C. section 1806(f). In its order, the Court determined that with respect to Plaintiffs' statutory claims under the Wiretap Act, 18 U.S.C. section 2511(1), and the Electronic Communications Privacy Act or Stored Communications Act, 18 U.S.C. section 2703, that 18 U.S.C. section 2712 waives sovereign immunity for damages claims. (*Id.* at 15-18.) The Court also specifically found that section 2712(b)(4) "designat[es] Section 1806(f) as 'the exclusive means by which materials [designated as sensitive by the government] shall be reviewed' in suits against the United States under FISA, the Wiretap Action, and the Electronic Privacy Protection Act." (Order dated July 23. 2013 at 13.)

The Court has reviewed the parties' briefing in response to the Court's questions in connection with earlier briefing. Considering the interim flux in relevant precedent and transitions in law, and having received no dispositive motion to adjudicate Plaintiffs' remaining statutory claims for damages, those claims are currently ripe for discovery. The procedural mechanism under 50 U.S.C. section 1806(f) of FISA serves to alleviate the risk of disclosure of state secret information.

The current state of the pleadings requires that the Court allow Plaintiffs to pursue their statutory claims for damages. The Ninth Circuit has explicitly cautioned this Court not to dispose of the issue of standing at the pleading stage. *See Jewel v. National Secuirity Agency*, 673 F.3d 902, 911 (9th Cir. 2011). Although "[u]ltimately Jewel may face ... procedural, evidentiary and substantive barriers ..., at this initial pleading stage, the allegations are deemed true and are presumed to 'embrace the 'specific facts' needed to sustain the complaint.'" *Id.* (citing *Lujan v. Nat'l Wildlife Fed.*, 497 U.S. 871, 888 (1990)). Particularly, in the area of their statutory claims, this Court has found that in the absence of sovereign immunity, Plaintiffs may state claims under the Wiretap Act and the Stored Communications Act. The Ninth Circuit has found in this matter that "Congress specifically envisioned plaintiffs challenging government surveillance under this statutory constellation." *Id.* at 913. As to Jewel's statutory claims, "injury required by Article III may exist solely by virtue of statutes creating legal rights, the invasion of which creates standing." *Id.* at 908 (citing *Lujan v. Nat'l Wildlife Fed.*, 504 U.S. 555, 578 (1992)).

Without a further dispositive determination of all of the remaining claims at issue at this time, the Court has found that Plaintiffs have sufficiently pled Counts 9, 12, and 15. Further, the Court has addressed the protective procedural mechanism by which any sensitive material may be reviewed. Although the Court has timely resolved all matters brought for resolution by the parties and the precedent in this area is in flux, the Court is mindful of the Ninth Circuit's directive to advance the conclusion of this litigation. Accordingly, the Court GRANTS Plaintiffs' motion to lift the stay of discovery on Counts 9, 12, and 15. The Court notes that any disputed materials that Defendants contend may potentially run the risk of impermissible

disclosure of state secret information may be disclosed *ex parte* for *in camera* review. To the extent the parties seek to resolve the remaining legal claims as a matter of law, the Court admonishes that the parties should seek resolution of all remaining matters by summary adjudication on the merits, with the benefit of any potentially available discovery.

IT IS SO ORDERED.

Dated: February 19, 2016

JEFFREY S. WHITE
UNITED STATES DISTRICT JUDGE

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

CAROLYN JEWEL, ET AL.,

Plaintiffs,

v.

NATIONAL SECURITY AGENCY, ET AL.,

Defendants.

No. C 08-04373 JSW

VIRGINIA SHUBERT, ET AL.,

Plaintiffs,

v.

BARACK OBAMA, ET AL.,

Defendants.

No. C 07-00693 JSW

ORDER DENYING PLAINTIFFS' MOTION FOR PARTIAL SUMMARY JUDGMENT AND GRANTING DEFENDANTS' MOTION FOR PARTIAL SUMMARY JUDGMENT

Now before the Court is the motion filed by Plaintiffs Carolyn Jewel, Erik Knutzen, and Joice Walton, on behalf of themselves and all other individuals similarly situated ("Plaintiffs") for partial summary judgment on their claim for relief which challenges the interception of their Internet communications as a violation of the Fourth Amendment ("Fourth Amendment Claim" or "Claim"). Also before the Court is the cross-motion for partial summary judgment on Plaintiffs' Fourth Amendment Claim filed by Defendants National Security Agency, United States Department of Justice, Barack H. Obama, Michael S. Rogers, Eric H. Holder, Jr., and James R. Clapper, Jr. (in their official capacities) (collectively, "Government Defendants").

Having considered the parties' papers, including the Government Defendants' classified brief and classified declarations, and the parties' arguments, the Court DENIES Plaintiffs'

motion for partial summary judgment and GRANTS the Government Defendants' cross-motion for partial summary judgment.[1]

The issues raised by the pending motions and additional briefing now before the Court compel the Court to examine serious issues, namely national security and the preservation of the rights and liberties guaranteed by the United States Constitution. The Court finds the predicament delicate and the resolution must strike a balance of those significant competing interests.

Based on the public record, the Court finds that the Plaintiffs have failed to establish a sufficient factual basis to find they have standing to sue under the Fourth Amendment regarding the possible interception of their Internet communications. Further, having reviewed the Government Defendants' classified submissions, the Court finds that the Claim must be dismissed because even if Plaintiffs could establish standing, a potential Fourth Amendment Claim would have to be dismissed on the basis that any possible defenses would require impermissible disclosure of state secret information.

BACKGROUND

Plaintiffs allege that as part of a system of mass surveillance, the Government Defendants receive copies of their Internet communications, then filter the universe of collected communications in an attempt to remove wholly domestic communications, and then search the remaining communications for search terms called "selectors" for potentially terrorist-related foreign intelligence information.

The Government has described the collection of communications pursuant to Section 702 of the Foreign Intelligence Surveillance Act ("Section 702") in several public reports. Upon approval by the Foreign Intelligence Surveillance Court of a certification under Section 702, NSA analysts identify non-U.S. persons located outside the United States who are reasonably believed to possess or receive, or are likely to communicate, foreign intelligence information designated in the certification. (*See, e.g.*, NSA Civil Liberties and Privacy Office

[1] Having not relied on Plaintiffs' proposed order submitted after the hearing on the motions, the Court DENIES Defendants' motion to strike it.

Report, NSA's Implementation of FISA Section 702 at 4 (Apr. 16, 2014) ("Civil Liberties Report")). Once designated by the NSA as a target, the NSA tries to identify a specific means by which the target communicates, such as an e-mail address or telephone number. That identifier is referred to a "selector." Selectors are only specific communications accounts, addresses, or identifiers. (*See id*; *see also* Privacy and Civil Liberties Oversight Board Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act ("PCLOB Report") at 32-33, 36.) According to the Government's admissions, an electronic communications service provider may then be compelled to provide the Government with all information necessary to acquire communications associated with the selector, a process called "tasking." (*Id.* at 32-33; *see also* Civil Liberties Report at 4-5.)

One process by which the NSA obtains information related to the tasked selectors is known as the Upstream collection program. Through a Section 702 directive, this program compels the assistance of the providers that control the telecommunications backbone within the United States. (*See* PCLOB Report at 35.) Under the Upstream collection program, tasked selectors are sent to domestic electronic communications service providers to acquire communications that transit the Internet backbone. (*See id.* at 36-37.) Internet communications are filtered in an effort to remove all purely domestic communications, and are then scanned to capture only those communications containing the designated tasked selectors. (*Id.* at 37.) "Unless [communications] pass both these screens, they are not ingested into governmental databases." (*Id.*)

Plaintiffs contend that the copying and searching of their private Internet communications is conducted without a warrant or any individualized suspicion and, accordingly, violates the Fourth Amendment. The Fourth Amendment prohibits the Government from intercepting, copying, or searching through communications without a warrant issued by a neutral and detached magistrate, upon probable cause, particularly describing the place to be searched and the things to be seized. Judicial warrants based on particularity and probable cause are especially crucial in electronic surveillance, where searches

and seizures occur without leaving a trace and where the threat to privacy is especially great. *United States v. U.S. District Court (Keith)*, 407 U.S. 297, 313 (1972).

In their motion for partial summary judgment, Plaintiffs seek adjudication as to their Fourth Amendment Claim with regard only to the NSA's acknowledged Upstream collection of communications pursuant to Section 702. The Government Defendants contend that Plaintiffs' evidence is insufficient to establish standing, and that even assuming standing, either there can be no Fourth Amendment violation on the facts in the record as a matter of law, or alternatively, that the state secrets privilege requires dismissal of Plaintiffs' Fourth Amendment Internet surveillance claim.

The Court shall address other additional specific facts as necessary in the remainder of this Order.

ANALYSIS

A. Summary Judgment Standard.

Summary judgment is appropriate when the record demonstrates "that there is no genuine issue as to any material fact and that the moving party is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(c). An issue is "genuine" if there is sufficient evidence for a reasonable fact finder to find for the non-moving party. *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248-49 (1986). "[A]t the summary judgment stage the judge's function is not . . . to weigh the evidence and determine the truth of the matter but to determine whether there is a genuine issue for trial." *Id.* at 249. A fact is "material" if it may affect the outcome of the case. *Id.* at 248. The party moving for summary judgment bears the initial responsibility of identifying those portions of the record which demonstrate the absence of a genuine issue of a material fact. *Celotex Corp. v. Catrett*, 477 U.S. 317, 323 (1986).

Once the moving party meets this initial burden, the non-moving party "may not rest upon the mere allegations or denials of the adverse party's pleading, but the adverse party's response, by affidavits or as otherwise provided in this rule, must set forth specific facts showing that there is a genuine issue for trial." Fed. R. Civ. P. 56(e). In the absence of such

facts, "the moving party is entitled to a judgment as a matter of law." *Celotex*, 477 U.S. at 323; *see also Keenan*, 91 F.3d at 1279.

B. Standing.

Defendants contend that Plaintiffs have not submitted evidence sufficient to establish that they have standing to challenge the alleged ongoing collection of communications by the NSA. As Defendants admit, the Government has acknowledged the existence of the Upstream collection process which involves the collection of certain communications as they transit the Internet backbone network of telecommunications service providers. However, the technical details of the collections process remain classified.

In order to prevail on their motion for summary judgment, Plaintiffs must support each element of their claim, including standing, "with the manner and degree of evidence required at the successive stages of the litigation." *Bras v. Cal. Pub. Utils. Comm'n*, 59 F.3d 869, 872 (9th Cir. 1995) (quoting *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561 (1992)). Plaintiffs must proffer admissible evidence establishing both their standing as well as the merits of their claims. *See* Fed. R. Civ. P. 56(c); *see also In re Oracle Corp. Sec. Litig.*, 627 F.3d 376, 385 (9th Cir. 2010) (holding that the court's ruling on summary judgment must be based only on admissible evidence). If Plaintiffs are unable to make a showing sufficient to establish an essential element of their claim on which they bear the burden at trial, summary judgment must be granted against them. *See Celotex Corp.*, 477 U.S. at 322.

"To establish Article III Standing, an injury must be 'concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling.'" *Clapper v. Amnesty International USA*, --- U.S. --- , 133 S. Ct. 1138, 1147 (2013) (quoting *Monsanto Co. v. Geertson Seed Farms*, 561 U.S. 139 (2010)). "Although imminence is concededly a somewhat elastic concept, it cannot be stretched beyond its purpose, which is to ensure that the alleged injury is not too speculative for Article III purposes – that the injury is *certainly* impending." *Id.* (citing *Lujan*, 504 U.S. at 565 n.2) (emphasis in original). Thus, the Supreme Court has "repeatedly reiterated that 'the threatened injury must be *certainly impending* to constitute injury in fact,' and that '[a]llegations of *possible* future injury' are not

sufficient." *Id.* (quoting *Whitmore v. Arkansas*, 495 U.S. 149, 158 (1990) (emphasis in original)).

In *Clapper*, the Court found that allegations that plaintiffs' communications were intercepted were too speculative, attenuated, and indirect to establish injury in fact that was fairly traceable to the governmental surveillance activities. *Id.* at 1147-50. The *Clapper* Court held that plaintiffs lacked standing to challenge NSA surveillance under FISA because their "highly speculative fear" that they would be targeted by surveillance relied on a "speculative chain of possibilities" insufficient to establish a "certainly impending" injury. *Id.*

Here, Plaintiffs have sufficiently demonstrated that they are AT&T customers. (*See* Declaration of Carolyn Jewel at ¶¶ 2-5; Declaration of Erik Knutzen at ¶¶ 2-6; Declaration of Joice Walton at ¶¶ 2-6.) In addition, Plaintiffs allege that, as AT&T customers, all of their Internet communications have been collected and amassed in storage. *See Hepting v. AT&T Corp.*, 439 F. Supp. 2d 974, 991-92 (N.D. Cal. 2006) ("AT&T and the government have for all practical purposes already disclosed that AT&T assists the government in monitoring communication content."). The record suggests that AT&T currently aids the Government in the collection of information transported over the Internet. (*See* AT&T Transparency Report dated 2014.) If the governmental program is sufficiently large and encompassing to include the mass collection of all Internet communications, the question of whether any specific communication was specifically targeted is not the relevant inquiry. *See Klayman v. Clapper*, 957 F. Supp. 2d 1, 26-28 (D.D.C. 2013) (granting standing to individual plaintiffs to challenge NSA collection of their telephone records from Verizon after finding "strong evidence" that NSA collected Verizon metadata for the last seven years and ran queries that necessarily analyzed that data); *see also Smith v. Obama*, 24 F. Supp. 3d 1005, 1007 n.2 (D. Idaho 2014) (finding that plaintiff, a Verizon customer, had standing to bring an action based on collection of telephone metadata). "As FISC Judge Eagan noted, the collection of virtually all telephony metadata is 'necessary' to permit the NSA, not the FBI, to do the algorithmic data analysis that allow the NSA to determine 'connections between known and unknown international terrorist operatives.'" *ACLU v. Clapper*, 959 F. Supp. 2d 724, 746 (S.D.N.Y. 2013) (citing *In re*

Application of the Fed. Bureau of Investigation for an Order Requiring the Prod. of Tangible Things from [REDACTED], amended clip op. at 22-23); *see also id.* at 748 ("[A]ggregated telephony metadata is relevant because it allows the querying technique to be comprehensive. . . . Armed with all the metadata, NSA can draw connections it might otherwise never be able to find.").

The creation of a large surveillance program designed to "intercept all or substantially all of its customers' communications, . . . necessarily inflicts a concrete injury that affects each customer in a distinct way, depending on the content of that customer's communications and the time that customer spends using AT&T services." *Hepting*, 439 F. Supp. 2d at 1001. In this matter, the Ninth Circuit has held that although the harm alleged by Plaintiffs is widely shared, that does not necessarily render it a generalized grievance. *See Jewel v. Nat'l Sec. Agency*, 783 F.3d 902, 909-10 (9th Cir. 2011) ("[W]e conclude that Jewel alleged a sufficiently concrete and particularized injury, Jewel's allegations are highly specific and lay out concrete harms arising from the warrantless searches."). Accordingly, the Court finds that, as Plaintiffs have provided evidence that they are AT&T customers who send Internet communications, they have crossed the threshold requirement to establish that, should the program work as alleged, their communications would be captured in a dragnet Internet collection program.

However, the question whether Plaintiffs can establish standing to pursue their Fourth Amendment claim against the Government Defendants for constitutional violations goes beyond whether they, as individuals and AT&T customers with Internet communications, can proffer evidence of generalized surveillance of Internet communications. Although the public and admissible evidence presented establishes that Plaintiffs are indeed AT&T customers with Internet communications and would fall into the class of individuals surveilled, the evidence at summary judgment is insufficient to establish that the Upstream collection process operates in the manner in which Plaintiffs allege it does.

In their attempt to establish the factual foundation for their standing to sue on their Fourth Amendment Claim, Plaintiffs rely in large part on the declarations of Mark Klein and their proffered expert, J. Scott Marcus, as well as other former AT&T and NSA employees to

present the relevant operational details of the surveillance program. Plaintiffs assert that the declarations support the contention that all AT&T customers' Internet communications are currently the subject of a dragnet seizure and search program, controlled by or at the direction of the Government. However, having reviewed the record in its entirety, the Court finds the Plaintiffs' evidence does not support this claim.

Plaintiffs principally rely on the declaration of Klein, a former AT&T technician who executed a declaration in 2006 about his knowledge and perceptions about the creation of a secure room at the AT&T facility at Folsom Street in San Francisco. However, the Court finds that Klein cannot establish the content, function, or purpose of the secure room at the AT&T site based on his own independent knowledge. *See* Fed. R. Civ. P. 56(c)(4). The limited knowledge that Klein does possess firsthand does not support Plaintiffs' contention about the actual operation of the Upstream data collection process. Klein can only speculate about what data were actually processed and by whom in the secure room and how and for what purpose, as he was never involved in its operation. In addition, Plaintiffs' expert, Marcus, relies exclusively on the observations and assumptions by Klein to formulate his expert opinion. Accordingly, his testimony about the purpose and function of the secure equipment at AT&T and assumed operational details of the program is not probative as it not based on sufficient facts or data. *See* Fed. R. Evid. 702(b). The Court finds that Plaintiffs have failed to proffer sufficient admissible evidence to support standing on their claim for a Fourth Amendment violation of interference with their Internet communications. In addition, without disclosing any of the classified content of the Government Defendants' submissions, the Court can confirm that the Plaintiffs' version of the significant operational details of the Upstream collection process is substantially inaccurate.

In addition, having reviewed the classified portion of the record, the Court concludes that even if the public evidence proffered by Plaintiffs were sufficiently probative on the question of standing, adjudication of the standing issue could not proceed without risking exceptionally grave damage to national security. The details of the Upstream collection process that are subject the Government's assertion of the state secrets privilege are necessary to

address the defenses against Plaintiffs' theory of standing as well as to engage in a full and fair adjudication of Government Defendants' substantive defenses against the Claim. The Court has reviewed the classified brief submitted by the Government and finds that its legal defenses are persuasive, and must remain classified.

Disclosure of this classified information would risk informing adversaries of the specific nature and operational details of the Upstream collection process and the scope of the NSA's participation in the program. Notwithstanding the unauthorized public disclosures made in the recent past and the Government's subsequent releases of previously classified information about certain NSA intelligence gathering activities since 2013, the Court notes that substantial details about the challenged program remain classified. The question of whether Plaintiffs have standing and the substantive issue of whether there are Fourth Amendment violations cannot be litigated without impinging on that heightened security classification. Because a fair and full adjudication of the Government Defendants' defenses would require harmful disclosures of national security information that is protected by the state secrets privilege, the Court must exclude such evidence from the case. *See Mohamed v. Jeppesen DataPlan, Inc.*, 614 F.3d 1070, 1083 (9th Cir. 2010) (holding that "application of the privilege may require dismissal" of a claim if, for example, "the privilege deprives the plaintiff of information needed to set forth a prima facie case, or the defendant of information that would otherwise give the defendant a valid defense to the claim"). Addressing any defenses involves a significant risk of potentially harmful effects any disclosures could have on national security. *See Kasza v. Browner*, 133 F.3d 1159, 1166 (9th Cir. 1998).

The Court is frustrated by the prospect of deciding the current motions without full public disclosure of the Court's analysis and reasoning. However, it is a necessary by-product of the types of concerns raised by this case. Although partially not accessible to the Plaintiffs or the public, the record contains the full materials reviewed by the Court. The Court is persuaded that its decision is correct both legally and factually and furthermore is required by the interests of national security.

CONCLUSION

For the foregoing reasons, the Court DENIES Plaintiffs' motion for partial summary judgment and GRANTS the Government Defendants' cross-motion for partial summary judgment regarding the allegations of Fourth Amendment violations challenging the possible interception of Plaintiffs' Internet communications.

IT IS SO ORDERED.

Dated: February 10, 2015

JEFFREY S. WHITE
UNITED STATES DISTRICT JUDGE

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

CAROLYN JEWEL, ET AL.,

Plaintiffs,

v.

NATIONAL SECURITY AGENCY, ET AL.,

Defendants.

No. C 08-04373 JSW

VIRGINIA SHUBERT, ET AL.,

Plaintiffs,

v.

BARACK OBAMA, ET AL.,

Defendants.

No. C 07-00693 JSW

AMENDED ORDER

In response to the parties' request for clarification, the Court issues this amended order. This matter comes before the Court upon consideration of the motion for partial summary judgment filed by Plaintiffs Carolyn Jewel, Tash Hepting, Young Boon Hicks, Erik Knutzen and Joice Walton, on behalf of themselves and all others similarly situated (collectively "*Jewel* Plaintiffs" or "Plaintiffs") and the cross motion to dismiss and for summary judgment filed by Defendants National Security Agency; Keith B. Alexander, Director of National Security Agency, in his official capacity; United States of America; Barack Obama, President of the United States, in his official capacity; the Department of Justice; Eric Holder, the Attorney General, in his official capacity; and James R. Clapper, Director of National Intelligence, in his official capacity (collectively "*Jewel* Defendants" or "Defendants").

This matter also comes before the Court in a related case upon consideration of the motion to dismiss and for summary judgment filed by Defendants Barack Obama, President of the United States, in his official capacity; Keith B. Alexander, Director of the National Security Agency, in his official capacity; the United States of America; and Eric Holder, the Attorney General, in his official capacity ("*Shubert* Defendants" or "Defendants") against Plaintiffs Virginia Shubert, Noha Arafa, Sarah Dranoff, and Hilary Botein, on behalf of themselves and all others similarly situated (collectively "*Shubert* Plaintiffs" or "Plaintiffs").

The *Jewel* Plaintiffs move for partial summary adjudication seeking to have the Court reject the Defendants' state secret defense by arguing that Congress has displaced the state secrets privilege in this action by the statutory procedure prescribed by 50 U.S.C. § 1806(f) of the Foreign Intelligence Surveillance Act ("FISA").

The *Shubert* Plaintiffs filed an amended complaint upon remand of the case and the *Shubert* Defendants move to dismiss for lack of subject matter jurisdiction on the basis that Congress did not waive sovereign immunity as to the FISA claim. The *Shubert* Plaintiffs incorporate by reference the arguments made in the *Jewel* Defendants' motion.

Defendants in both related cases move to dismiss all of Plaintiffs' statutory claims for lack of subject matter jurisdiction on the basis that Congress did not waive sovereign immunity as to the statutory claims. Defendants also move for summary judgment on all counts on the grounds that Plaintiffs' claims would risk or require the disclosure of certain information that is properly protected by the statutory protections and the state secrets privilege asserted in this action by the Director of National Intelligence and by the National Security Agency.

Having thoroughly considered the parties' papers, Defendants' public and classified declarations, the relevant legal authority and the parties' arguments, the Court GRANTS the *Jewel* Plaintiffs' motion for partial summary adjudication by rejecting the state secrets defense as having been displaced by the statutory procedure prescribed in 50 U.S.C. § 1806(f) of FISA. In both related cases, the Court GRANTS Defendants' motions to dismiss Plaintiffs' statutory claims for damages as to FISA and claims for injunctive relief as to all statutory claims on the basis of sovereign immunity. The Court further finds that the parties have not addressed the

viability of the *Jewel* Plaintiffs' constitutional claims under the Fourth and First Amendments and the claim for violation of separation of powers and the *Shubert* Plaintiffs' fourth cause of action for violation of the Fourth Amendment. Accordingly, the Court RESERVES ruling on Defendants' motion for summary judgment on those remaining, non-statutory claims.

The Court shall require that the parties submit further briefing on the course of this litigation going forward.[1]

BACKGROUND

These cases are two in a series of many lawsuits arising from claims that the federal government, with the assistance of major telecommunications companies, conducted widespread warrantless dragnet communications surveillance of United States citizens following the attacks of September 11, 2001. Plaintiffs filed these putative class actions on behalf of themselves and a class of similarly situated persons described as "millions of ordinary Americans . . . who use[] the phone system or the Internet" and "a class comprised of all present and future United States persons who have been or will be subject to electronic surveillance by the National Security Agency without a search warrant or court order since September 12, 2001." (*Jewel* Complaint at ¶¶ 1, 7, and 9; *see also Shubert* Complaint at ¶ 1, 2, 20.)[2]

According to the allegations in the *Jewel* Complaint, a program of dragnet surveillance (the "Program") was first authorized by Executive Order of the President on October 4, 2001. (*Jewel* Complaint at ¶¶ 3, 39.) Plaintiffs allege that, in addition to eavesdropping on or reading specific communications, Defendants have "indiscriminately intercepted the communications content and obtained the communications records of millions of ordinary Americans as part of the Program authorized by the President." (*Id.* at ¶ 7.) The core component of the Program is a

[1] The Court DENIES Defendants' request for a stay of this decision. The subject matter and legal questions presented by this lawsuit are timely. To the extent recent events involving the public disclosure of relevant, and previously classified, information bear on the future course of the litigation, the Court shall require that the parties submit further briefing to address these issues.

[2] For the remaining facts, the Court refers to the *Jewel* Complaint as it is more inclusive. The facts pertinent to the Court's analysis are also similarly alleged in the related *Shubert* Complaint which was originally filed May 17, 2006, as part of a multi-district litigation action also remanded to this Court.

nationwide network of sophisticated communications surveillance devices attached to the key facilities of various telecommunications companies that carry Americans' Internet and telephone communications. (*Id.* at ¶¶ 8, 42.) Plaintiffs allege that Defendants have unlawfully solicited and obtained the private telephone and internal transactional records of millions of customers of the telecommunications companies, including records indicating who the customers communicated with, when those communications took place and for how long, among other sensitive information. Plaintiffs allege these records include both domestic and international communications. (*Id.* at ¶ 10.) Plaintiffs sue Defendants "to enjoin their unlawful acquisition of the communications and records of Plaintiffs and class members, to require the inventory and destruction of those that have already been seized, and to obtain appropriate statutory, actual, and punitive damages to deter future illegal surveillance." (*Id.* at ¶ 14.)

The *Jewel* Plaintiffs allege seventeen counts against Defendants for: violation of the Fourth Amendment (counts 1 and 2); violation of the First Amendment (counts 3 and 4); violation of FISA, 50 U.S.C. §§ 1809, 1810 (counts 5 and 6); violation of the Wiretap Act, 18 U.S.C. § 2511(1)(a), (b), and (d) (counts 7 through 9); violation of the Electronic Communications Privacy Act or the Stored Communications Act, 18 U.S.C. § 2703(a), (b), and (c) (counts 10 through 15); violation of the Administrative Procedure Act, 5 U.S.C. § 701 *et seq.* (count 16); and violation of separation of powers (count 17). The *Shubert* Plaintiffs allege four causes of action for violations of FISA, the Wiretap Act, the Stored Communications Act, and the Fourth Amendment.

The *Jewel* Complaint was originally filed on September 18, 2008. Defendants moved to dismiss and alternatively sought summary judgment as to all claims. Defendants contended that the Court lacked jurisdiction over the statutory claims because the government had not waived its sovereign immunity. Defendants moved for summary judgment on the remaining claims based on the argument that the information necessary to litigate the claims was properly subject to the state secrets privilege. The district court dismissed the claims without leave to amend based on its finding that Plaintiffs failed to make out the *prima facie* allegations necessary to establish standing.

On appeal, the Ninth Circuit Court of Appeals reversed the district court's dismissal of the *Jewel* Complaint on standing grounds. The Ninth Circuit Court of Appeals remanded "with instructions to consider, among other claims and defenses, whether the government's assertion that the state secrets privilege bars this litigation." *Jewel v. National Security Agency*, 673 F.3d 902, 913-14 (9th Cir. 2011). Upon remand, Plaintiffs filed their motion for partial summary adjudication urging the Court to reject Defendants' state secret defense. Defendants cross-moved to dismiss on the basis of sovereign immunity for the statutory claims and for summary judgment on the assertion of the state secrets privilege.

The Court will address additional facts as necessary in the remainder of this Order.

ANALYSIS

A. Applicable Legal Standards.

1. Motion to Dismiss.

A motion to dismiss is proper under Federal Rule of Civil Procedure 12(b)(6) where the pleadings fail to state a claim upon which relief can be granted. The Court's "inquiry is limited to the allegations in the complaint, which are accepted as true and construed in the light most favorable to the plaintiff." *Lazy Y Ranch Ltd. v. Behrens*, 546 F.3d 580, 588 (9th Cir. 2008). Even under the liberal pleading standard of Federal Rule of Civil Procedure 8(a)(2), "a plaintiff's obligation to provide the 'grounds' of his 'entitle[ment] to relief' requires more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do." *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 555 (2007) (citing *Papasan v. Allain*, 478 U.S. 265, 286 (1986)). Pursuant to *Twombly*, a plaintiff must not merely allege conduct that is conceivable but must instead allege "enough facts to state a claim to relief that is plausible on its face." *Id.* at 570. "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (citing *Twombly*, 550 U.S. at 556).

2. Motion for Summary Judgment.

A principal purpose of the summary judgment procedure is to identify and dispose of factually unsupported claims. *Celotex Corp. v. Cattrett*, 477 U.S. 317, 323-24 (1986). Summary judgment is proper when the "pleadings, depositions, answers to interrogatories, and admissions on file, together with the affidavits, if any, show that there is no genuine issue as to any material fact and that the moving party is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(a). "In considering a motion for summary judgment, the court may not weigh the evidence or make credibility determinations, and is required to draw all inferences in a light most favorable to the non-moving party." *Freeman v. Arpaio*, 125 F.3d 732, 735 (9th Cir. 1997).

The party moving for summary judgment bears the initial burden of identifying those portions of the pleadings, discovery, and affidavits that demonstrate the absence of a genuine issue of material fact. *Celotex*, 477 U.S. at 323; *see also* Fed. R. Civ. P. 56(c). An issue of fact is "genuine" only if there is sufficient evidence for a reasonable fact finder to find for the non-moving party. *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248-49 (1986). A fact is "material" if it may affect the outcome of the case. *Id.* at 248. Once the moving party meets its initial burden, the non-moving party must go beyond the pleadings and, by its own evidence, "set forth specific facts showing that there is a genuine issue for trial." Fed. R. Civ. P. 56(e).

In order to make this showing, the non-moving party must "identify with reasonable particularity the evidence that precludes summary judgment." *Keenan v. Allan*, 91 F.3d 1275, 1279 (9th Cir. 1996) (quoting *Richards v. Combined Ins. Co.*, 55 F.3d 247, 251 (7th Cir. 1995) (stating that it is not a district court's task to "scour the record in search of a genuine issue of triable fact"); *see also* Fed. R. Civ. P. 56(e). If the non-moving party fails to point to evidence precluding summary judgment, the moving party is entitled to judgment as a matter of law. *Celotex*, 477 U.S. at 323; Fed. R. Civ. P. 56(e)(3).

B. State Secrets Privilege.

The state secrets privilege is a common law privilege that permits the government to bar the disclosure of information if "there is a reasonable danger" that disclosure will "expose

military matters which, in the interest of national security, should not be divulged." *United States v. Reynolds*, 345 U.S. 1, 10 (1953). The state secrets privilege strikes a delicate balance "between fundamental principles of our liberty, including justice, transparency, accountability and national security." *Mohamed v. Jeppesen Dataplan, Inc.*, 614 F.3d 1070, 1073 (9th Cir. 2010).

The state secrets privilege has two applications: as a rule of evidentiary privilege, barring only the secret evidence from exposure during litigation, and as a rule of non-justiciability, when the subject matter of the lawsuit is itself a state secret, necessitating dismissal. *See ACLU v. National Security Agency*, 493 F.3d 644, 650 n.2 (6th Cir. 2007). The first application of evidentiary withholding can serve to remove only certain specific pieces of evidence or can be applied to compel the removal of a sufficiently broad swath of evidence which then has the consequence of requiring dismissal of the entire suit. Such a dismissal may be necessitated by the instances in which the removal of evidence disables a plaintiff from the ability to establish the *prima facie* elements of a claim without resort to privileged information or instances in which the removed evidence bars the defendant from establishing a defense. *See Kasza v. Browner*, 133 F.3d 1159, 1166 (9th Cir. 1998).

The analysis of whether the state secrets privilege applies involves three distinct steps. First, the Court must ascertain whether the procedural requirements for invoking the privilege have been satisfied. Second, the Court must make an independent determination whether the information is privileged. In determining whether the privilege attaches, the Court may consider a party's need for access to the allegedly privileged materials. *See Reynolds*, 345 U.S. at 11. Lastly, the "ultimate question to be resolved is how the matter should proceed in light of the successful privilege claim." *El-Masri v. United States*, 479 F.3d 296, 304 (4th Cir. 2007).

With regard to the first step, to ascertain whether the procedural requirements have been met, the assertion of the privilege belongs exclusively to the government. The head of the department which has control over the matter must properly assert a formal and timely claim of privilege, after actual personal consideration by that officer. *See Reynolds*, 345 U.S. at 7-8. Such an invocation must be made only after "serious, considered judgment, not simply [as] an

administrative formality." *United States v. W.R. Grace*, 526 F.3d 499, 507-08 (9th Cir. 2008) (en banc). "The formal claim must reflect the certifying official's personal judgment ... [and] must be presented in sufficient detail for the court to make an independent determination of the validity of the claim of privilege and the scope of the evidence subject to the privilege." *Jeppesen*, 614 F.3d at 1080.

Second, the reviewing court must "make an independent determination whether the information is privileged." *Al-Haramain*, 507 F.3d at 1202. The court must "sustain a claim of privilege when it is satisfied, 'from all the circumstances of the case, that there is a reasonable danger that compulsion of the evidence will expose . . . matters which, in the interest of national security, should not be divulged.'" *Jeppesen*, 614 F.3d at 1081 (quoting *Reynolds*, 345 U.S. at 10). In making this determination, the Court must strike the appropriate balance "between protecting national security matters and preserving an open court system." *Al-Haramain*, 507 F.3d at 1203. "This inquiry is a difficult one, for it pits the judiciary's search for truth against the Executive's duty to maintain the nation's security." *El-Masri*, 479 F.3d at 304. In evaluating the need for secrecy, the court must defer to the Executive on matters of foreign policy and national security. *See Jeppesen*, 614 F.3d at 1081-82. However, the assertion of the state secrets doctrine does not "represent a complete surrender of judicial control over access to the courts." *El-Masri*, 479 F.3d at 312. Rather, in order to ensure that the doctrine is not asserted more frequently and sweepingly than necessary, "it is essential that the courts continue critically to examine instances of its invocation." *Ellsberg v. Mitchell*, 709 F.2d 51, 58 (D.C. Cir. 1983). However, should the court find that the materials must not be divulged, "the evidence is absolutely privileged, irrespective of the plaintiffs' countervailing need for it." *See Jeppeson*, 614 F.3d at 1081 (citing *Reynolds*, 345 U.S. at 11).

Lastly, the third step in the analysis requires that the court determine how the matter should proceed once it has sustained a claim of privilege. "The court must assess whether it is feasible for the litigation to proceed without the protected evidence and, if so, how." *Jeppesen*, 614 F.3d at 1082. When the government successfully invokes the state secrets privilege, "the evidence is completely removed from the case." *Kasza*, 133 F.3d at 1166. The court is then

tasked with disentangling the nonsensitive information from the privileged evidence. Often, after the privileged evidence is excluded, "the case will proceed accordingly, with no consequences save those resulting from the loss of evidence." *Al-Haramain*, 507 F.3d at 1204 (quoting *Ellsberg*, 709 F.3d at 64). However, there "will be occasions when, as a practical matter, secret and nonsecret information cannot be separated. In some cases, therefore, 'it is appropriate that the courts restrict the parties' access not only to evidence which itself risks the disclosure of a state secret, but also those pieces of evidence or areas of questioning which press so closely upon highly sensitive material that they create a high risk of inadvertent or indirect disclosures.'" *Jeppesen*, 614 F.3d at 1082 (quoting *Bareford v. Gen. Dynamics Corp.*, 973 F.2d 1138, 1143-44 (5th Cir. 1992); *see also Kasza*, 133 F.3d at 1166 ("[I]f seemingly innocuous information is part of a . . . mosaic, the state secrets privilege may be invoked to bar its disclosure and the court cannot order the government to disentangle this information from other [*i.e.*, secret] information.")

Thereafter, the case may proceed with the omission of the secret or closely entangled evidence. Alternatively, if application of the state secrets bars too much, the court may be required to dismiss the action in its entirety. Such instances include when, without the secret evidence, a plaintiff is unable to prove the *prima facie* elements of a claim with nonprivileged evidence. *See Kasza*, 133 F.3d at 1166. Or the privilege may apply to bar information that would otherwise give the defendant a valid defense to the claim, thus requiring dismissal. *See id.* Lastly, the court may be compelled to dismiss when, although the claims and defenses may be stated without reference to privileged evidence, "it may be impossible to proceed with the litigation because – privileged evidence being inseparable from nonprivileged information that will be necessary to the claims or defenses – litigating the case to a judgment on the merits would present an unacceptable risk of disclosing state secrets." *Jeppesen*, 614 F.3d at 1083 (citations omitted); *see also Farnsworth Cannon, Inc. v. Grimes*, 635 F.2d 268, 279-80 (4th Cir. 1980) (en banc) (per curiam) (Phillips, J., specially concurring and dissenting) (concluding that "litigation should be entirely foreclosed at the outset by dismissal of the action" if it appears that "the danger of inadvertent compromise of the protected state secrets outweighs the public

and private interests in attempting formally to resolve the dispute while honoring the privilege").

Alternatively, the state secrets privilege may be invoked to bar litigation of the matter in its entirety where "the trial of which would inevitably lead to the disclosure of matters which the law itself regards as confidential, and respecting which it will not allow the confidence to be violated." *Totten v. United States*, 92 U.S. 105, 107 (1875). Where the very subject matter of the lawsuit is a matter of state secret, the action must be dismissed without reaching the question of evidence. *See Al-Haramain*, 507 F.3d at 1197 (citations omitted); *see also Sterling v. Tenet*, 416 F.3d 338, 345 (4th Cir. 2005) (holding that dismissal is proper where "sensitive military secrets will be so central to the subject matter of the litigation that any attempt to proceed will threaten disclosure of the privileged matters.")

Here, having reviewed the materials submitted for review and having considered the claims alleged and the record as a whole, the Court finds that Defendants have timely invoked the state secrets doctrine. Defendants contend that Plaintiffs' lawsuits should be dismissed as a result of the application of the privilege because the state secrets information is so central to the subject matter of the suit that permitting further proceedings would jeopardize national security. Given the multiple public disclosures of information regarding the surveillance program, the Court does not find that the very subject matter of the suits constitutes a state secret. Just as in *Al-Haramain*, and based significantly on the same set of facts in the record here, the Court finds that although there are certainly details that the government has not yet disclosed,

> because of the voluntary disclosures made by various officials since December 2005, the nature and purpose of the [Terrorist Surveillance Program], the 'type' of persons it targeted, and even some of its procedures are not state secrets. In other words, the government's many attempts to assuage citizens' fears that they have not been surveilled now doom the government's assertion that the very subject matter of this litigation, the existence of a warrantless surveillance program, is barred by the state secrets privilege.

507 F.3d at 1200; *see also Hepting v. AT&T Corp.*, 439 F. Supp. 2d 974, 986-88, 991 (N.D. Cal. 2006) (holding that the existence of a program of monitoring the contents of certain telephone communications was no longer a state secret as a result of the public statements made by the President and the Attorney General). Accordingly, the Court does not find dismissal

appropriate based on the subject matter of the suits being a state secret. *See Totten*, 92 U.S. at 107.

However, here, the Court finds there would be significant evidence that would be properly excluded should the case proceed. The Court has thoroughly and critically reviewed Defendants' public and classified declarations and is persuaded that the evidence submitted thus far that the government seeks to protect from disclosure contain valid state secrets "which, in the interest of national security, should not be divulged." *Reynolds*, 345 U.S. at 10; *see also Terkel v. AT&T Corp.*, 441 F. Supp. 2d 899, 917 (N.D. Ill. 2006) (finding state secrets privilege applies because requiring the telephone company to confirm or deny whether it had disclosed large quantities of telephone records to the federal government could give adversaries valuable insight into the government's intelligence programs and "requiring such disclosures would therefore adversely affect our national security" and "are barred by the state secrets privilege"). The Court finds the state secrets privilege would apply to bar disclosure of significant materials relating to the alleged Program. However, it may not set out precisely which matters the privilege covers lest the Court jeopardize the secrets it is bound to protect. *See Jeppesen*, 614 F.3d at 1086 (citing *Black v. United States*, 62 F.3d 1115, 1119 (8th Cir. 1995) ("Care in protecting state secrets is necessary not only during a court's review of the evidence, but in its subsequent treatment of the question in any holding; a properly phrased opinion should not strip the veil from state secrets even if ambiguity results in a loss of focus and clarity.")).

Having concluded that Defendants have successfully invoked the state secrets privilege with regard to significant evidence tending to confirm or negate the factual allegations in Plaintiffs' complaints, the question the Court must address is how to proceed. If the state secrets defense applies to bar disclosure altogether of much of the evidence sought in this suit, Plaintiffs may neither be able to establish standing to sue nor state a *prima facie* case. Defendants would similarly be without accessible evidence to establish a defense without disclosure of the evidence subject to the privilege. *See Kasza*, 133 F.3d at 1166. However, the Court finds that, as a matter of law, the FISA procedural mechanism prescribed under 50 U.S.C. § 1806(f) preempts application of the state secrets privilege.

C. FISA and Preemption.

On remand, the Court of Appeals has required this Court to consider "the government's assertion that the state secrets privilege bars this litigation." *Jewel*, 673 F.3d at 913-14. The Ninth Circuit, in a previous matter relating to the Program, also remanded to the district court to consider "whether FISA preempts the state secrets privilege and for any proceedings collateral to that determination." *Al-Haramain*, 507 F.3d at 1206. In its opinion on remand in the *Al-Haramain* matter, this district court found that "FISA preempts the state secrets privilege in connection with electronic surveillance for intelligence purposes . . . ." *In re National Security Agency Telecommunications Records Litigation* ("*In re N.S.A. Telecommunication Records Litig.*"), 564 F. Supp. 2d 1109, 1111 (N.D. Cal. 2008). The undersigned agrees and finds that the *in camera* review procedure in FISA applies and preempts the determination of evidentiary preclusion under the state secrets doctrine. Section 1806(f) of FISA displaces the state secrets privilege in cases in which electronic surveillance yields potentially sensitive evidence by providing secure procedures under which courts can consider national security evidence that the application of the state secrets privilege would otherwise summarily exclude.

1. FISA.

Congress enacted FISA to curb the problem of unchecked domestic surveillance and intelligence-gathering abuses undertaken by the executive branch in the post-World War II era. *See* S. Rep. No. 95-604, at 8 (Congress enacted FISA in response to "revelations that warrantless surveillance in the name of national security ha[d] been seriously abused."). The misconduct was exposed by a Congressional task force known as the Church Committee, which produced a series of investigative reports documenting unlawful surveillance pursued in the name of national security. The Church Committee concluded that "the massive record of intelligence abuses over the years" had "undermined the constitutional rights of citizens . . . primarily because checks and balances designed by the framers of the Constitution to assure accountability have not been applied." *Book II: Intelligence Activities and the Rights of Americans*, S. Rep. No. 94-755, at 291. Accordingly, the Committee urged "fundamental

reform," that would "cover[] the field by . . . provid[ing] the exclusive legal authority for domestic security activities," including "warrantless electronic surveillance." *Id.* at 299.

Under FISA, before engaging in domestic surveillance, the Executive branch must seek authorization from a special court charged with finding probable cause that the target is an agent of a foreign power as defined by the statute. *See* 50 U.S.C. §§ 1804-05. FISA also establishes a system of review of Executive conduct by setting out specific procedures courts must follow to evaluate evidence where disclosure could endanger national security. *See* 50 U.S.C. § 1806(f).

Section 1806(f) reads in pertinent part:

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

Id.

Section 1806(f) of FISA applies "notwithstanding any other law" and is the "exclusive" procedure for reviewing sensitive surveillance materials gathered by the Executive under FISA and other surveillance statutes. *See id.*; *see also* 18 U.S.C. § 2712(b)(4) (designating Section 1806(f) as "the exclusive means by which materials [designated as sensitive by the government] shall be reviewed" in suits against the United States under FISA, the Wiretap Act, and the Electronic Privacy Protection Act). Once invoked, the review procedure requires courts to review the potentially sensitive surveillance materials *ex parte* and *in camera*. 50 U.S.C. § 1806(f).

The purpose of this provision is to permit courts to determine whether any particular surveillance was lawfully authorized and executed. The provision, which permits courts to review the potentially sensitive materials, strikes a balance between executive action and judicial oversight. The legislative history makes clear that Congress intended to formulate a balanced legislative solution to the national security problems raised in litigation over possibly

unlawful executive surveillance programs. The Senate Judiciary Committee explained that litigants were not to evade the provision by invoking other laws or jurisprudential doctrines:

> The Committee wishes to make clear that the procedures set in [subsection 1806(f)] apply whatever the underlying rule or statute referred to in [a party's] motion. This is necessary to prevent the carefully drawn procedures in [section 1806(f)] from being bypassed by the inventive litigant using a new statute, rule or judicial construction.

S. Rep. No. 95-604, at 57; *see also* S. Rep. No. 95-701, at 63 ("When the procedure is so triggered, however, the Government must make available to the court a copy of the court order and accompanying declaration upon which the surveillance was based."); *see also* H. Rep. No. 95-1283(I), at 91 (when the legality of surveillance is at issue, "it is this procedure 'notwithstanding any other law' that must be used to resolve the question").

2. Preemption.

Based on the legislative history and the plain language of FISA, this Court finds that FISA preempts the common law doctrine of the state secrets privilege. Federal common law applies "[u]ntil the field has been made the subject of comprehensive legislation." *City of Milwaukee v. Illinois and Michigan*, 451 U.S. 304, 314 (1981). When it passed FISA, Congress expressly indicated its intention to replace judge-made federal common law rules:

> [T]he development of the law regulating electronic surveillance for national security purposes has been uneven and inconclusive. This is to be expected where the development is left to the judicial branch in an area where cases do not regularly come before it. Moreover, the development of standards and restrictions by the judiciary with respect to electronic surveillance for foreign intelligence purposes accomplished through case law threatens both civil liberties and the national security because the development occurs generally in ignorance of the facts, circumstances, and techniques of foreign intelligence electronic surveillance not present in the particular case before the court . . . . [T]he tiny window to this area which a particular case affords provides inadequate light by which judges may be relied upon to develop case law which adequately balances the rights of privacy and national security.

H. Rep. No. 95-1283, at 21.

It is clear Congress intended for FISA to displace federal common law rules such as the state secrets privilege with regard to matters within FISA's purview. The legislative history indicates that Congress intended to "occupy the field through the establishment of a comprehensive regulatory program supervised by an expert administrative agency." *Milwaukee*, 452 U.S. at 317. Through explicit provisions of FISA, Congress "established a

comprehensive, detailed program to regulate foreign intelligence surveillance in the domestic context." *In re N.S.A. Telecommunications Records Litig.*, 564 F. Supp. 2d at 1118. In particular, § 1806(f) "is Congress's specific and detailed description 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. The specific description leaves no room for application of the state secrets privilege and is, in effect, a "codification of the state secrets privilege for purposes of relevant cases under FISA, 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.* The Court agrees that "FISA preempts or displaces the state secrets privilege, but only in cases within the reach of its provisions." *Id.* at 1124. As in *In re National Security Agency Telecommunications Records Litigation*, Plaintiffs' allegations here of warrantless wiretapping and surveillance programs similarly fall within those provisions.

However, because the Court finds that Defendants have not waived sovereign immunity for its statutory claim, Plaintiffs' claims for violation of FISA fail.

D. Waiver of Sovereign Immunity for Plaintiffs' Statutory Claims.

Defendants also move to dismiss Plaintiffs' statutory claims on the grounds that sovereign immunity has not been waived. "Absent a waiver, sovereign immunity shields the Federal Government and its agencies from suit." *F.D.I.C. v. Meyer*, 510 U.S. 471, 475 (1994); *see also United States v. Mitchell*, 463 U.S. 206, 212 (1983) ("It is axiomatic that the United States may not be sued without its consent and that the existence of consent is a prerequisite for jurisdiction."). Plaintiffs bear the burden to establish a waiver of sovereign immunity. *Prescott v. United States*, 973 F.2d 696, 701 (9th Cir. 1992)

1. Statutory Claims for Damages.

Plaintiffs bring statutory claims for damages under FISA, the Wiretap Act, and the Stored Communications Act ("SCA"). Section 223 of the Patriot Act amended the SCA and added the following provision which waives sovereign immunity for three specific provisions of FISA and more generally for violations of the SCA and the Wiretap Act.

> Any person who is aggrieved by any willful violation of this chapter or of chapter 119 of this title or of sections 106(a), 305(a), or 405(a) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 *et seq*.) may commence an action in United States District Court against the United States to recover money damages.

18 U.S.C. § 2712. *See* Pub. L. No. 107-56 § 223, 115 Stat. 272 (2001).

Plaintiffs do not bring any claims under these three enumerated provisions of FISA. Plaintiffs sue Defendants for violating 50 U.S.C. § 1809, and they rely on 50 U.S.C. § 1810 to provide a waiver of sovereign immunity in order to sue for damages. However, as Plaintiffs concede, the Ninth Circuit has explicitly rejected the proposition that § 1810 may be construed as a waiver of sovereign immunity to sue for damages. *See Al-Haramain v. Obama*, 690 F.3d 1089 (9th Cir. 2012) (holding that 50 U.S.C. § 1810 does not waive sovereign immunity against the United States for damages). Therefore, Plaintiffs' claim for damages under FISA against the United States and against the individual federal defendants in their official capacity is barred.

However, the waiver of sovereign immunity for damages claims against the United States contained with Section 2712 for claims under the SCA and the Wiretap Act is much broader. While the waiver in Section 2712 is limited to three specific provisions of FISA, the waiver for claims under the SCA and the Wiretap Act is not similarly restricted to individual provisions within those statutes. Nevertheless, Defendants contend that the waiver is limited to claims under the SCA and the Wiretap Act for the use and disclosure of information obtained from electronic surveillance, not just its collection. Defendants argue that plain language and the legislative history of Section 223 of the Patriot Act supports this limitation. The Court finds this argument unpersuasive.

In construing the provisions of a statute, courts must "first look to the language of the statute to determine whether it has a plain meaning." *Satterfield v. Simon & Schuster, Inc.*, 569 F.3d 946, 951 (9th Cir. 2009); *see also United States v. Chaney*, 581 F.3d 1123, 1126 (9th Cir. 2009) ("It is well settled that statutory interpretation begins with the plain language of the statute.") (internal quotation marks and citation omitted). "The preeminent canon of statutory interpretation requires us to presume that [the] legislature says in a statute what it means and

means in a statute what it says there. Thus, our inquiry begins with the statutory text, and ends there as well if the text is unambiguous." *McDonald v. Sun Oil Co.*, 548 F.3d 774, 780 (9th Cir. 2008) (quoting *BedRoc Ltd., LLC v. United States*, 541 U.S. 176, 183 (2004)) (internal quotation marks omitted).

The plain language of Section 2712(a) does not limit the waiver of sovereign immunity for damage claims under the SCA and the Wiretap Act to claims for the use and disclosure of information. In Section 2712(a), Congress specifically limited the waiver for damage claims to three specific sections of FISA and easily could have done the same with respect to the Wiretap Act and the SCA. The fact that Congress did not similarly limit the waiver to specific sections within the Wiretap Act and the SCA has significance. To ignore this distinction would be to ignore the plain language and structure of the statute. *Cf. TRW Inc. v. Andrews*, 534 U.S. 19, 31 (2001) ("It is a cardinal principle of statutory construction that a statute ought, upon the whole, to be so construed that, if it can be prevented, no clause, sentence, or word shall be superfluous, void, or insignificant.") (internal quotation marks and citation omitted); *United States v. Novak*, 476 F.3d 1041, 1048 (9th Cir. 2007) ("We avoid whenever possible statutory interpretations that result in superfluous language.").

Defendants argue that reading Section 223 of the Patriot Act as a whole demonstrates that the waiver of sovereign immunity by Section 2712(a) is limited to claims regarding the use and disclosure of information. In support of this argument, Defendants rely upon the fact that Section 223 was titled "Civil Liability for Certain Unauthorized Disclosures" and upon the fact that other provisions of Section 223 specifically addressed claims for the use and disclosure of information. However, the Court finds this argument unpersuasive. Neither the title of the Section 223, nor the fact that Section 223 includes additional provisions that address claims regarding the use and disclosure of information, alters the clear and unambiguous statutory language. Again, the Court emphasizes that Section 2712 explicitly limits the waiver to specific provisions of FISA and does not limit the waiver to specific provisions within the Wiretap Act or the SCA. If Congress intended to limit the waiver to claims regarding the use and disclosure claims within all three statutes, it could have done so. The Court cannot ignore the fact that

Congress chose to do so with respect to one of these statutes and did not with respect to the other two. *See Botosan v. Paul McNally Realty*, 216 F.3d 827, 832 (9th Cir. 2000) ("The incorporation of one statutory provision to the exclusion of another must be presumed intentional under the statutory canon of *expressio unius*.")

Next, Defendants invite the Court to read limitations into the waiver of sovereign immunity from the legislative history of this statutory provision. "[E]ven where the plain language appears to settle the question, we may nonetheless look to the legislative history to determine whether there is clearly expressed legislative intention contrary to that language that overcomes the strong presumption that Congress has expressed its intent in the language it chose." *Amalgamated Transit Union Local 1309, AFL-CIO v. Laidlaw Transit Services, Inc.*, 435 F.3d 1140, 1146 (9th Cir. 2006). In addition, the Ninth Circuit has stated that the "plain meaning rule . . . does not require a court to operate under an artificially induced sense of amnesia about the purpose of legislation, or to turn a blind eye towards significant evidence of Congressional intent in the legislative history." *Amalgamated Transit Union Local 1309, AFL-CIO v. Laidlaw Transit Services, Inc.*, 448 F.3d 1092, 1093 (9th Cir. 2006) (quoting *Heppner v. Aleyeska Pipeline Serv. Co.*, 665 F.2d 868, 871 (9th Cir. 1981)). Upon review of the legislative history, the Court does not find "clearly expressed legislative intention contrary to that language that overcomes the strong presumption that Congress has expressed its intent in the language it chose." *Amalgamated Transit Union*, 435 F.3d at 1146. Accordingly, the Court finds that Section 2712 waives sovereign immunity for Plaintiffs' claims for damages under the Wiretap Act and the SCA.

2. Statutory Claims for Injunctive Relief.

Section 2712 is inapplicable to Plaintiffs' claims for injunctive relief. Section 2712 only applies to claims for damages. Therefore, Plaintiffs must turn elsewhere to establish a waiver of sovereign immunity. To do so, Plaintiffs rely on Section 702 of the Administrative Procedure Act ("APA") and on the common law *ultra vires* exception set forth in *Larson v. Domestic & Foreign Commerce Corporation*, 337 U.S. 682 (1949).

a. The Administrative Procedures Act.

Section 702 of the APA provides:

> A person suffering legal wrong because of agency action, or adversely affected or aggrieved by agency action within the meaning of a relevant statute, is entitled to judicial review thereof. An action in a court of the United States seeking relief other than money damages and stating a claim that an agency or an officer or employee thereof acted or failed to act in an official capacity or under color of legal authority shall not be dismissed nor relief therein be denied on the ground that it is against the United States or that the United States is an indispensable party . . . . Nothing herein (1) affects other limitations on judicial review or the power or duty of the court to dismiss any action or deny relief on any other appropriate legal or equitable ground; or (2) confers authority to grant relief if any other statute that grants consent to suit expressly or impliedly forbids the relief which is sought.

5 U.S.C § 702. Defendants contend that Section 702 is inapplicable because it does not "confer[] authority to grant relief if any other statute that grants consent to suit expressly or impliedly forbids the relief which is sought." *See id.* Defendants argue that Section 223 of the Patriot Act is such a statute.

"'[W]hen Congress has dealt in particularity with a claim and [has] intended a specified remedy' – including its exceptions – to be exclusive, that is the end of the matter; the APA does not undo the judgment." *Match-E-Be-Nash-She-Wish Band of Pottawatomi Indians v. Patchak*, --- U.S. ---, 132 S. Ct. 2199, 2205 (2012) (quoting *Block v. North Dakota ex rel. Board of Univ. and School Lands*, 461 U.S. 273, 286, n.22 (1976)) ("*Pottawatomi Indians*"). Section 223 of the Patriot Act amended the Wiretap Act, the SCA, and FISA to allow suits against the United States for damages. The question presented here is whether, by granting authority to sue the United States for damages, the Patriot Act impliedly limited the authority to sue the United States for other types of relief, such as injunctive or declaratory relief. The Court finds that it does.

With respect to the SCA and the Wiretap Act, Section 223 of the Patriot Act not only granted consent to sue the United States for damages, but it also explicitly deleted the United States from the provisions that permit an aggrieved person to sue for recovery and obtain relief, including "preliminary and other equitable or declaratory relief." *See* Pub. L. No. 107–56 § 223, 115 Stat. 272 (2001) (amending 18 U.S.C. § 2520(a) and 18 U.S.C. § 2707(a) to insert

"other than the United States"). Therefore, the Court finds the intent of Congress in passing Section 223 of the Patriot Act was to forbid injunctive and declaratory relief against the United States under the SCA and the Wiretap Act.

Although the additional evidence on Congressional intent regarding the SCA and the Wiretap Act noted above is lacking, the Court finds that the Patriot Act must still be read to restrict the authority to sue the United States to suits for damages for the three specific statutory provisions listed in § 2712. Significantly, any ambiguities must be read in favor of the United States' immunity from suit. *See Federal Aviation Administration v. Cooper*, --- U.S. ---, 132 S. Ct. 1441, 1448 (2012) ("Any ambiguities in the statutory language are to be construed in favor of immunity . . . ."). Moreover, the Court notes that the Patriot Act's grant of authority to sue under FISA is more restricted than the grant of authority to sue under the Wiretap Act and the SCA. Thus, it would be inconsistent to hold that the waiver of sovereign immunity is broader with respect to FISA than to the Wiretap Act and the SCA.

Relying on *Pottawatomi Indians*, Plaintiffs argue that the exception to the waiver of sovereign immunity in Section 702 does not bar their FISA claim for injunctive relief because they are "bringing a different claim, seeking different relief" from the specific FISA provisions listed in § 2712(a). 132 S. Ct. at 2209. Plaintiffs' reliance on this case is misplaced. In *Pottawatomi Indians*, the Court held that the ban on bringing suit under the Quiet Title Act ("QTA") did not apply because the plaintiff was not bringing a claim under that statute. *Id*. at 2208 (finding that the plaintiff was "not bringing a QTA suit at all"). Here, Plaintiffs indisputably bring claims under FISA. Thus, the issue is whether FISA, by allowing suits against the United States only for damages based on three provisions of that statute, impliedly bans suits against the United States that seek injunctive relief under any provision of FISA. The Court finds that it does. Accordingly, Plaintiffs cannot rely on Section 702 of the APA for a waiver of sovereign immunity.

b. The *Ultra Vires* Doctrine.

Next, Plaintiffs seek to invoke the *ultra vires* exception to sovereign immunity of federal officials as set forth in *Larson*. Under this doctrine, "[i]f an employee of the United States acts

completely outside of his governmental authority, he has no immunity." *United States v. Yakima Tribal Court* ("*Yakima Tribal Court*"), 806 F.2d 853, 859 (9th Cir. 1986); *see also Larson*, 337 U.S. at 689-90.

There is some question as to whether this doctrine survived the 1976 amendments to the APA. The Ninth Circuit has commented that "Congress observed that before the amendment to Section 702 [of the APA], litigants seeking . . . non-monetary relief were forced to resort to the 'legal fiction' of naming individual officers, rather than the government, as defendants, . . . an approach that was 'illogical' and 'becloud[ed] the real issue whether a particular governmental activity should be subject to judicial review, and, if so, what form of relief is appropriate.'" *See The Presbyterian Church (U.S.A.) v. United States*, 870 F.2d 518, 524 (9th Cir. 1989) (quoting H. Rep. No. 1656, at 5, *reprinted in* 1976 U.S. Code Cong. & Admin. News 6121, 6125, 6128-29). The Ninth Circuit found it "significant that Congress referred disapprovingly to the *Ex parte Young* fiction, which permitted a plaintiff to name a government official as the defendant in equitable actions to redress government misconduct, on the pretense that the suit was not actually against the government." *Id*. at 525-26 (citing *Larson*, 337 U.S. at 689-91). The Circuit Court stated that "Congress' plain intent in amending Section 702 was to waive sovereign immunity for all such suits, thereby eliminating the need to invoke the *Young* fiction." *Id.* at 526; *see also Equal Employment Opportunity Commission v. Peabody Western Coal Co.*, 610 F.3d 1070, 1085 (9th Cir. 2010) (noting that in *Presbyterian Church (U.S.A.)*, the Circuit Court "explained that after § 702 was amended in 1976, it replaced the *Ex parte Young* fiction as the doctrinal basis for a claim for prospective relief[]" and that "since 1976 federal courts have looked to § 702 of the [APA] to serve the purposes of the *Ex parte Young* fiction in suits against federal officers.")

Nevertheless, there is case law in the Ninth Circuit, post-dating the amendments to the APA in 1976, that applies the *ultra vires* doctrine or at least suggests its continued existence. *See, e.g., Yakima Tribal Court*, 806 F.2d at 859 ("If an employee of the United States acts completely outside his governmental authority, he has no immunity.") (citing *Larson*, 337 U.S. at 689); *De Lao v. Califano*, 560 F.2d 1384, 1391 (9th Cir. 1977) (noting that courts have

recognized two exceptions to sovereign immunity when suits are brought against government officials, including the *ultra vires* doctrine). The Ninth Circuit has declined to address whether the *ultra vires* doctrine set forth in *Larson* exists in light of the wavier provided by Section 702 of the APA and has noted that the decisions in this area are "hopelessly inconsistent." *Beller v. Middendorf*, 632 F.2d 788, 797 (9th Cir. 1980), *overruled on other grounds* by *Bowers v. Hardwick*, 478 U.S. 186 (1986). While noting the confusion, the Ninth Circuit declined to attempt a reconciliation. *Id.* In the absence of clear authority holding that the *ultra vires* doctrine is no longer viable, the Court will not dismiss Plaintiffs' statutory claims for injunctive relief to the extent they are premised on the *ultra vires* doctrine because the 1976 amendments to the APA invalidated this doctrine.

However, to the extent the *ultra vires* doctrine survives, its scope is quite narrow. First, the Court notes that an *ultra vires* claim may only be asserted against officers in their individual or personal capacity. *See Larson*, 337 U.S. at 687-89. Moreover, a claim that an officer was acting *ultra vires* "is different from the situation where an employee acting as a government agent, commits an act that is arguably a mistake of fact or law." *Yakima Tribal Court*, 806 F.2d at 859. An "[u]ltra vires claim[] rest[s] on the official's lack of delegated authority." *Id*. at 860. As the Supreme Court explained in the context of addressing the viability of the *ultra vires* doctrine against state officials, the *ultra vires* exception to sovereign immunity is "very narrow." *Pennhurst State School & Hosp. v. Halderman*, 465 U.S. 89, 114 n.25 (1984). An officer "may be said to act *ultra vires* only when he acts 'without any authority whatever.'" *Id*. at 102 n.11 (quoting *Florida Dept. of State v. Treasure Salvors, Inc.*, 458 U.S. 670, 697, 716 (1982)) (White, J., concurring in judgment in part and dissenting in part) (finding that the test is whether there was no "colorable basis for the exercise of authority by state officials"). "[A]n *ultra vires* claim rests on 'the officer's lack of delegated power. A claim of error in the exercise of that power is therefore not sufficient.'" *Id*. (quoting *Larson*, 337 U.S. at 690).

In *Pennhurst*, the trial court's undisputed findings were that the residents of the state facility were "often physically abused or drugged by staff members . . . ." *Pennhurst*, 465 U.S. at 92. The Supreme Court held that the "[p]etitioners' actions in operating [the] mental health

institution plainly were not beyond their delegated authority" and that the "essence" of the respondents' claims was that the petitioners failed to provide services adequately. *Id*. at 102 n.11.

Here, it is undisputed that Defendants have authority to conduct electronic surveillance. In their claims for declaratory, injunctive and other equitable relief, Plaintiffs contend that Defendants conducted electronic surveillance improperly, without following the proper procedures, and in violation of FISA, the Wiretap Act and the SCA. In essence, Plaintiffs contend that the individual defendants erred in their exercise of their authority to conduct electronic surveillance. Such a claim does not fit within the narrow exception to sovereign immunity under the *ultra vires* doctrine.

The fact that Plaintiffs are challenging a government-wide "program" bolsters the Court's conclusion that Plaintiffs may not proceed under the narrow *ultra vires* exception. "[T]he key question in addressing the sovereign immunity of the United States is 'whether the relief sought in a suit nominally addressed to the officer is relief against the sovereign.'" *Aminoil U.S.A., Inc. v. California State Water Resources Control Board*, 674 F.2d 1227, 1234 (9th Cir. 1982) (quoting *Larson*, 337 U.S. at 687). Here, Plaintiffs seek to obtain relief from the sovereign itself, under the guise of suing officials individually. Plaintiffs allege that beginning in early October 2011, then-President Bush, in concert with the other individual defendants, authorized "a range of surveillance activities inside of the United States without any statutory authorization or court approval." (*Jewel* Complaint at ¶ 39.) Plaintiffs label this alleged activity as "the Program." (*Id*.; *see also Jewel* Complaint at ¶ 42 ("The Program of domestic surveillance authorized by the President and conducted by Defendants . . . ."). Plaintiffs seek to halt this alleged governmental "Program." Plaintiffs cannot obtain effective relief from "the Program" by suing Defendants individually.[3]

[3] The Court's conclusion that Defendants are essentially seeking relief from the Government is further bolstered by the fact that Plaintiffs have not substituted in the current officials whom they seek to sue in their official capacity. Pursuant to Federal Rule of Civil Procedure 25, an action against an officer in her or her official capacity does not abate when that officer ceases to hold office while the action is pending. Instead, "[t]he officer's successor is automatically substituted as a party." *See* Fed. R. Civ. P. 25(d). Although the

The Court concludes that Plaintiffs' statutory claims for injunctive relief may not proceed under the *ultra vires* doctrine. Therefore, the Court finds that sovereign immunity has not been waived and grants Defendants' motion to dismiss on Plaintiffs' statutory claims for injunctive relief.

CONCLUSION

For the foregoing reasons, the Court GRANTS Plaintiffs' motion for partial summary adjudication by rejecting the state secrets defense as having been displaced by the statutory procedure prescribed in 50 U.S.C. § 1806(f) of FISA. The Court GRANTS Defendants' motions to dismiss Plaintiffs' claims for damages under FISA and all statutory claims for injunctive relief on the basis of sovereign immunity. The Court RESERVES ruling on the Defendants' motions for summary judgment on remaining non-statutory claims (counts 1-4 of the *Jewel* Complaint and the fourth cause of action in the *Shubert* Complaint).

The Court shall require that the parties submit briefing on both the scope of FISA preemption on the Plaintiffs' constitutional claims, specifically, whether the scope of the preemption only provides a procedural mechanism for the review of submitted evidentiary materials or whether the scope of FISA preemption is broader to foreclose altogether the substantive constitutional claims. Should the Court permit the constitutional claims to proceed and find that § 1806(f) merely provides the mechanism for review of submitted materials, Plaintiffs shall be tasked with the burden to establish standing to sue without resulting in impermissible damage to ongoing national security efforts. *See Clapper v. Amnesty International USA*, 133 S. Ct. 1138, 1149 n.4 (2013) (noting that, pursuant to hypothetical *in camera* proceedings permitted under § 1806(f), "the court's postdisclosure decision about

---

text of Rule 25 applies only to actions against officers in their official capacity, Plaintiffs rely on the notes to the amendment to Rule 25 in 1961. The notes provide that "[t]he amended rule will apply to all actions brought by public officers for the government..." and to "actions to prevent officers from acting in excess of their authority or under authority not validly conferred...." *See* Fed. R. Civ. P. 25. Advisory Committee's Notes (citing *Ex parte Young*, 209 U.S. 123). The advisory committee explain that the Rule "will apply whenever effective relief would call for corrective behavior by the one then having official status and power, rather than one who has lost that status and power through ceasing to hold office." *Id*. (citing *Larson*, 337 U.S. at 682). Because the notes do provide that the officers' successors will be substituted in automatically when they are sued under the *ultra vires* doctrine as set forth in *Ex parte Young* and *Larson*, the Court substitutes in the current office holders.

whether to dismiss the suit for lack of standing would surely signal to the terrorist whether his name was on the list of surveillance targets.") Although the Court finds, at this procedural posture, that Plaintiffs here do not allege the attenuated facts of future harm which barred standing in *Clapper*, the potential risk to national security may still be too great to pursue confirmation of the existence or facts relating to the scope of the alleged governmental Program.

Further, the Court shall require briefing on the impact on the Defendants' assertion of such a risk following the recent disclosure of the government's continuing surveillance activities and the statement by the Director of National Intelligence that certain information related to the "business records" provision of FISA should be declassified and immediately released to the public.

In order to facilitate this process and set the schedule for such further briefing, the Court shall conduct a case management conference on August 23, 2013 at 1:30 p.m. The parties shall submit a joint case management statement by no later than August 16, 2013.

IT IS SO ORDERED.

Dated: July 23, 2013

JEFFREY S. WHITE
UNITED STATES DISTRICT JUDGE