

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

IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF CALIFORNIA

CAROLYN JEWEL, ET AL.,

Plaintiffs,

No. C 08-04373 JSW

v.

NATIONAL SECURITY AGENCY, ET AL.,

Defendants.

\_\_\_\_\_

VIRGINIA SHUBERT, ET AL.,

Plaintiffs,

No. C 07-00693 JSW

v.

BARACK OBAMA, ET AL.,

Defendants.

**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’

1 motion for partial summary judgment and GRANTS the Government Defendants' cross-motion  
2 for partial summary judgment.<sup>1</sup>

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

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

### 15 BACKGROUND

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

21 The Government has described the collection of communications pursuant to Section  
22 702 of the Foreign Intelligence Surveillance Act ("Section 702") in several public reports.  
23 Upon approval by the Foreign Intelligence Surveillance Court of a certification under Section  
24 702, NSA analysts identify non-U.S. persons located outside the United States who are  
25 reasonably believed to possess or receive, or are likely to communicate, foreign intelligence  
26 information designated in the certification. (*See, e.g.*, NSA Civil Liberties and Privacy Office

---

27  
28 <sup>1</sup> Having not relied on Plaintiffs' proposed order submitted after the hearing on the motions, the Court DENIES Defendants' motion to strike it.

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

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

21 Plaintiffs contend that the copying and searching of their private Internet  
22 communications is conducted without a warrant or any individualized suspicion and,  
23 accordingly, violates the Fourth Amendment. The Fourth Amendment prohibits the  
24 Government from intercepting, copying, or searching through communications without a  
25 warrant issued by a neutral and detached magistrate, upon probable cause, particularly  
26 describing the place to be searched and the things to be seized. Judicial warrants based on  
27 particularity and probable cause are especially crucial in electronic surveillance, where searches  
28

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

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

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

## 12 ANALYSIS

### 13 A. Summary Judgment Standard.

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

24 Once the moving party meets this initial burden, the non-moving party "may not rest  
25 upon the mere allegations or denials of the adverse party's pleading, but the adverse party's  
26 response, by affidavits or as otherwise provided in this rule, must set forth specific facts  
27 showing that there is a genuine issue for trial." Fed. R. Civ. P. 56(e). In the absence of such  
28

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

3 **B. Standing.**

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

10 In order to prevail on their motion for summary judgment, Plaintiffs must support each  
11 element of their claim, including standing, “with the manner and degree of evidence required at  
12 the successive stages of the litigation.” *Bras v. Cal. Pub. Utils. Comm’n*, 59 F.3d 869, 872 (9th  
13 Cir. 1995) (quoting *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561 (1992)). Plaintiffs must  
14 proffer admissible evidence establishing both their standing as well as the merits of their claims.  
15 *See Fed. R. Civ. P. 56(c)*; *see also In re Oracle Corp. Sec. Litig.*, 627 F.3d 376, 385 (9th Cir.  
16 2010) (holding that the court’s ruling on summary judgment must be based only on admissible  
17 evidence). If Plaintiffs are unable to make a showing sufficient to establish an essential element  
18 of their claim on which they bear the burden at trial, summary judgment must be granted against  
19 them. *See Celotex Corp.*, 477 U.S. at 322.

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

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

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

9 Here, Plaintiffs have sufficiently demonstrated that they are AT&T customers. (*See*  
10 Declaration of Carolyn Jewel at ¶¶ 2-5; Declaration of Erik Knutzen at ¶¶ 2-6; Declaration of  
11 Joice Walton at ¶¶ 2-6.) In addition, Plaintiffs allege that, as AT&T customers, all of their  
12 Internet communications have been collected and amassed in storage. *See Hepting v. AT&T*  
13 *Corp.*, 439 F. Supp. 2d 974, 991-92 (N.D. Cal. 2006) (“AT&T and the government have for all  
14 practical purposes already disclosed that AT&T assists the government in monitoring  
15 communication content.”). The record suggests that AT&T currently aids the Government in  
16 the collection of information transported over the Internet. (*See* AT&T Transparency Report  
17 dated 2014.) If the governmental program is sufficiently large and encompassing to include the  
18 mass collection of all Internet communications, the question of whether any specific  
19 communication was specifically targeted is not the relevant inquiry. *See Klayman v. Clapper*,  
20 957 F. Supp. 2d 1, 26-28 (D.D.C. 2013) (granting standing to individual plaintiffs to challenge  
21 NSA collection of their telephone records from Verizon after finding “strong evidence” that  
22 NSA collected Verizon metadata for the last seven years and ran queries that necessarily  
23 analyzed that data); *see also Smith v. Obama*, 24 F. Supp. 3d 1005, 1007 n.2 (D. Idaho 2014)  
24 (finding that plaintiff, a Verizon customer, had standing to bring an action based on collection  
25 of telephone metadata). “As FISC Judge Eagan noted, the collection of virtually all telephony  
26 metadata is ‘necessary’ to permit the NSA, not the FBI, to do the algorithmic data analysis that  
27 allow the NSA to determine ‘connections between known and unknown international terrorist  
28 operatives.’” *ACLU v. Clapper*, 959 F. Supp. 2d 724, 746 (S.D.N.Y. 2013) (citing *In re*

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

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

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

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



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

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

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



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

5 Disclosure of this classified information would risk informing adversaries of the specific  
6 nature and operational details of the Upstream collection process and the scope of the NSA's  
7 participation in the program. Notwithstanding the unauthorized public disclosures made in the  
8 recent past and the Government's subsequent releases of previously classified information about  
9 certain NSA intelligence gathering activities since 2013, the Court notes that substantial details  
10 about the challenged program remain classified. The question of whether Plaintiffs have  
11 standing and the substantive issue of whether there are Fourth Amendment violations cannot be  
12 litigated without impinging on that heightened security classification. Because a fair and full  
13 adjudication of the Government Defendants' defenses would require harmful disclosures of  
14 national security information that is protected by the state secrets privilege, the Court must  
15 exclude such evidence from the case. *See Mohamed v. Jeppesen DataPlan, Inc.*, 614 F.3d 1070,  
16 1083 (9th Cir. 2010) (holding that "application of the privilege may require dismissal" of a  
17 claim if, for example, "the privilege deprives the plaintiff of information needed to set forth a  
18 prima facie case, or the defendant of information that would otherwise give the defendant a  
19 valid defense to the claim"). Addressing any defenses involves a significant risk of potentially  
20 harmful effects any disclosures could have on national security. *See Kasza v. Browner*, 133  
21 F.3d 1159, 1166 (9th Cir. 1998).

22 The Court is frustrated by the prospect of deciding the current motions without full  
23 public disclosure of the Court's analysis and reasoning. However, it is a necessary by-product  
24 of the types of concerns raised by this case. Although partially not accessible to the Plaintiffs or  
25 the public, the record contains the full materials reviewed by the Court. The Court is persuaded  
26 that its decision is correct both legally and factually and furthermore is required by the interests  
27 of national security.  
28

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

**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

**United States District Court**  
For the Northern District of California