CINDY COHN (SBN 145997)
cindy@eff.org
LEE TIEN (SBN 148216)
KURT OPSAHL (SBN 191303)
JAMES S. TYRE (SBN 083117)
MARK RUMOLD (SBN 279060)
ANDREW CROCKER (SBN 291596)
DAVID GREENE (SBN 160107)
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
Fax: (415) 436-9993

RICHARD R. WIEBE (SBN 121156)
wiebe@pacbell.net
LAW OFFICE OF RICHARD R. WIEBE
One California Street, Suite 900
San Francisco, CA 94111
Telephone: (415) 433-3200
Fax: (415) 433-6382

RACHAEL E. MENY (SBN 178514)
rmeny@kvn.com
BENJAMIN W. BERKOWITZ (SBN 244441)
MICHAEL S. KWUN (SBN 198945)
AUDREY WALTON-HADLOCK (SBN 250574)
JUSTINA K. SESSIONS (SBN 270914)
PHILIP J. TASSIN (SBN 287787)
KEKER & VAN NEST, LLP
633 Battery Street
San Francisco, CA 94111
Telephone: 415/391-5400; Fax: 415/397-7188

THOMAS E. MOORE III (SBN 115107)
tmoore@rroyselaw.com
ROYSE LAW FIRM, PC
1717 Embarcadero Road
Palo Alto, CA 94303
Telephone: 650/813-9700; Fax: 650/813-9777

ARAM ANTARAMIAN (SBN 239070)
aram@eff.org
LAW OFFICE OF ARAM ANTARAMIAN
1714 Blake Street
Berkeley, CA 94703
Telephone: (510) 289-1626

Counsel for Plaintiffs

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

CAROLYN JEWEL, TASH HEPTING, YOUNG BOON HICKS, as executrix of the estate of GREGORY HICKS, ERIK KNUTZEN and JOICE WALTON, on behalf of themselves and all others similarly situated,

Plaintiffs,

v.

NATIONAL SECURITY AGENCY, *et al.*,

Defendants.

Case No.: 4:08-cv-4373-JSW

[*REVISED* PROPOSED] ORDER GRANTING PLAINTIFFS CAROLYN JEWEL, ERIK KNUTZEN, AND JOICE WALTON'S MOTION FOR PARTIAL SUMMARY JUDGMENT (ECF No. 261) AND DENYING THE GOVERNMENT DEFENDANTS' CROSS-MOTION FOR PARTIAL SUMMARY JUDGMENT (ECF No. 286)

(Fourth Amendment Violation)

Courtroom 5, Second Floor
The Honorable Jeffrey S. White

[Plaintiffs Carolyn Jewel, Erik Knutzen, and Joice Walton, by their counsel Richard R. Wiebe and their other counsel of record, respectfully submit the following revised proposed order for the assistance of the Court in light of the hearing in this matter held on December 19, 2014.]

This matter comes before the Court on the motion of plaintiffs Carolyn Jewel, Erik Knutzen, and Joice Walton (collectively, "plaintiffs") for partial summary judgment challenging the ongoing interception of their Internet communications as a violation of the Fourth Amendment, and the cross-motion of 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, the "government defendants" or "the government") for partial summary judgment.[1]

In summary, plaintiffs have put forward evidence that as part of a system of mass surveillance their Internet communications are copied and provided to the government ("stage one"), which filters them in an attempt to remove wholly domestic communications ("stage two"), and which then searches the remaining communications for numerous search terms called "selectors" ("stage three"). Plaintiffs contend that the copying and searching of their communications is conducted without a warrant or any individualized suspicion and violates the Fourth Amendment. The government defendants have not put forward any public evidence disputing plaintiffs' evidence. Instead, they contend that plaintiffs' evidence is insufficient to establish plaintiffs' standing, that even assuming the sufficiency of plaintiffs' evidence there can be no Fourth Amendment violation on these facts as a matter of law, and, alternatively, that the state secrets privilege requires dismissal of plaintiffs' Fourth Amendment Internet surveillance claim.

Having considered the parties' papers (including the government defendants' classified brief and classified declarations) and the parties' arguments, the Court GRANTS plaintiffs' motion for partial summary judgment and DENIES the government defendants' cross-motion for partial

[1] Plaintiffs Tash Hepting and Young Boon Hicks (as executrix of the estate of Gregory Hicks) are not AT&T Internet customers and are not parties to this motion.

summary judgment. The Court holds that the government defendants' warrantless and suspicionless seizure of plaintiffs' Internet communications violates the Fourth Amendment, and that the government defendants' warrantless and suspicionless content-searching of plaintiffs' Internet communications violates the Fourth Amendment.

ANALYSIS

A. The Summary Judgment Legal Standard

"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* [*Corp.v. Catrett*], 477 U.S. [317,] at 323, 106 S. Ct. 2548 [(1986)]; *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 nonmoving party. *Anderson v. Liberty Lobby, Inc.,* 477 U.S. 242, 248-49, 106 S. Ct. 2505, 91 L.Ed.2d 202 (1986). A fact is 'material' if it may affect the outcome of the case. *Id.* at 248, 106 S. Ct. 2505. 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) [*see* current Rule 56(c)].

"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) [*see* current Rule 56(c)]. 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, 106 S. Ct. 2548; Fed. R. Civ. P. 56(e)(3)." *Jewel v. National Security Agency*, 965 F. Supp. 2d 1090, 1099-1100 (N.D. Cal. 2013).

Plaintiffs' motion raises the legal issues of whether the government's copying of plaintiffs' Internet communications at stage one is a seizure; whether the government's searching of those communications at stage three is a search; and, if there is a search or seizure, whether the search or seizure violates the Fourth Amendment. The government's cross-motion additionally puts at issue whether plaintiffs have established their standing by showing their communications have been

copied and searched, and whether the state secrets privilege requires dismissal of plaintiffs' Fourth Amendment claim regarding the search and seizure of their Internet communications.

The parties begin with some common ground. First, the parties agree for purposes of this motion that plaintiffs have a reasonable expectation of privacy in their Internet communications, including not just their emails, instant messages, and video chats but also their Internet browsing and social media posting and viewing. 12/19/14 Reporter's Transcript ("RT") at 75, 84, 94-96. Second, the parties agree that plaintiffs have a possessory interest in their Internet communications. *Id*. Third, the parties agree that if the Court reaches the merits of the Fourth Amendment issue, it must decide the case based solely on the public evidence and disregard the secret filings made by the government. 12/19/14 RT at 25-27, 42-45, 47.

B. The Factual Record

Plaintiffs present the following evidence in support of their allegations that the government is copying and searching their Internet communications.

The government admits that it is currently conducting ongoing surveillance intercepting communications transiting the Internet "backbone." These admissions include statements made in the *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* by the Privacy and Civil Liberties Oversight Board ("PCLOB Report"), statements in declassified declarations filed in this lawsuit, and statements to Congress.[2]

[2] *See, e.g.*, ECF No. 262, Ex. A (PCLOB Report) at 7, 35-37 (at 36-37: "Once tasked, selectors used for the acquisition of upstream Internet transactions are sent to a United States electronic communication service provider to acquire communications that are transiting through circuits that are used to facilitate Internet communications, what is referred to as the 'Internet backbone.' The provider is compelled to assist the government in acquiring communications across these circuits. To identify and acquire Internet transactions associated with the Section 702-tasked selectors on the Internet backbone, Internet transactions are first filtered to eliminate potential domestic transactions, and then are screened to capture only transactions containing a tasked selector."); ECF No. 227 (12/20/13 NSA Deputy Dir. Fleisch Classified Decl.) at ¶ 38, p. 25:14-16 ("NSA collects electronic communications with the compelled assistance of electronic communications service providers as they transit Internet 'backbone' facilities within the United States"); ECF No. 169 (12/20/13 NSA Deputy Dir. Fleisch Unclassified Decl.) at ¶ 29, p. 17; ECF No. 253-3 ("The Intelligence Community's Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act") at 3-4 ("NSA collects telephone and electronic communications as they transit the Internet 'backbone' within the United States. This is known as 'upstream' collection").

The government further admits that, as part of the process of surveillance, it filters communications transiting the Internet backbone in an attempt to eliminate wholly domestic communications and then content-searches the remaining communications to see whether they contain any one or more of many different selectors the government chooses to search for.[3] The government admits that this Internet backbone surveillance has been ongoing since 2001.[4]

AT&T in turn admits that it currently conducts Foreign Intelligence Surveillance Act (FISA) surveillance of communications content on behalf of the government.[5]

The declaration of Mark Klein and accompanying AT&T documents show the mass, indiscriminate copying of Internet communications of AT&T customers and other Internet users transiting links between AT&T's Internet backbone network and the rest of the Internet, as well as the delivery of those copies to the National Security Agency's ("NSA's") possession in a limited-access room controlled by the NSA in AT&T's facility (the "SG3 Secure Room").[6] The copying is

---

[3] *See*, *e.g.*, ECF No. 262, Ex. A (PCLOB Report) at 36-37, 121-22; ECF No. 310, Ex. A (PCLOB Report) at 38-41; ECF No. 172-8 (9/11/12 Classified Declaration of Frances J. Fleisch) at ¶ 69.

[4] ECF No. 310, Ex. A (PCLOB Report) at 5-6, 16-20.

[5] ECF No. 295, Ex. B (AT&T Transparency Report).

[6] ECF No. 84-2 (Klein Decl.) at ¶¶ 12, 19-20, 22, 24-36; ECF No. 84-3 (Klein Decl., Ex. A); ECF No. 84-4 (Klein Decl., Ex. B); ECF Nos. 84-5 & 84-6 (Klein Decl., Ex. C).

The Court overrules the government's personal-knowledge and hearsay objections to Klein's testimony. Klein's testimony regarding the copying of plaintiffs' communications by means of splitters and the transmission of those communications to the SG3 Secure Room is squarely within his personal knowledge, for his duties included operating and maintaining that equipment. *Barthelemy v. Air Lines Pilots Ass'n*, 897 F.2d 999, 1018 (9th Cir. 1990). So, too, is Klein's knowledge of AT&T's relationship with the NSA, including NSA's control over the copies sent to the SG3 Secure Room. Employees are routinely permitted to testify, as matters within their personal knowledge, to the activities of their employer, their supervisors, and co-workers, including the relationship between their employer and government agencies or other outside entities. *United States v. Neal*, 36 F.3d 1190, 1206 (1st Cir. 1994) (bank employee could testify to information she learned in the course of her job, including the status of the bank's relationship with a federal agency (the Federal Deposit Insurance Corporation) and the locations of its customers, even though her knowledge was based solely on hearsay statements in documents she reviewed); *DIRECTV, Inc. v. Budden*, 420 F.3d 521, 529 (5th Cir. 2005) (employee could testify about facts concerning another company he learned from a law enforcement investigation); *Great American Assurance Co. v. Liberty Surplus Ins. Corp.*, 669 F. Supp. 2d 1084, 1089 (N.D. Cal. 2009) (*footnote continued on following page*)

done by means of "splitters" that indiscriminately copy all the data flowing over fiber-optic cables.[7] The declaration of AT&T's James Russell attests that Klein's descriptions and the descriptions in the AT&T documents of the splitter equipment and the equipment in the SG3 Secure Room controlled by the NSA are accurate.[8] The declaration of plaintiffs' expert J. Scott Marcus explains the functionality of the splitters and the equipment in the SG3 Secure Room controlled by the NSA, and he opines that AT&T would have had no business purpose for using the splitters and the equipment in the SG3 Secure Room.[9]

(*footnote continued from preceding page*)
(employee can testify to company policies based on her "experience and perceptions" on the job); *Sjoblom v. Charter Communications, LLC*, 571 F. Supp. 2d 961, 968-69 (W.D. Wis. 2008) (employees may testify about the activities of their supervisors and co-workers that they observe); *United States v. Wirtz*, 357 F. Supp. 2d 1164, 1169-70 (D. Minn. 2005) (employee could testify that employees of a different company provided certain information and documents to his company even though he had no personal contact with the employees of the other company).

The government's hearsay objection fails for two separate reasons even if it is assumed AT&T's relationship with the NSA is not within Klein's personal knowledge. First, the statements made to Klein by management and other AT&T employees about the NSA's activities and the SG3 Secure Room are admissible nonhearsay. AT&T is the agent of the government in assisting the government in electronic surveillance, and statements by an agent on a matter within the scope of the agency relationship are admissible nonhearsay. Fed. R. Evid. 801(d)(2)(D); *Anestis v. United States*, __ F. Supp. 3d __, 2014 WL 4928959, at *4 n.3 (E.D. Ky. Sept. 30, 2014); *Quintero v. United States*, 2014 WL 201608, at *2 (D. Mass. Jan. 15, 2014); *Cefalu v. Holder*, 2013 WL 5315079, at *14 n.16 (N.D. Cal. Sept. 23, 2013); *L-3 Communications Integrated Systems v. United States*, 91 Fed. Cl. 347, 359 (Fed. Cl. 2010); *Globe Savings Bank, F.S.B. v. United States*, 61 Fed. Cl. 91, 93-95 (Fed. Cl. 2004). AT&T's statements in its transparency report and the NSA Inspector General's draft report (discussed in footnote 10 below) are independent evidence of the agency relationship. In addition to being admissible under Rule 801(d)(2)(D), the e-mail to Klein from AT&T management and statements by his manager and a co-worker telling of upcoming visits by an NSA agent (ECF No. 84-2 at ¶¶ 10, 16 (Klein Decl.)), are also admissible under Rule 803(3) as evidence that AT&T employees actually met with NSA agents for the purpose of implementing the surveillance, that AT&T's management's plan and intent was to cooperate with the NSA in implementing the surveillance, and that AT&T thereafter did cooperate with the NSA. Fed. R. Evid. 803(3) (statements reflecting plan or intent are admissible); *United States v. Best*, 219 F.3d 192, 198 (2d Cir. 2000) (statement of plan or intent can be used to "prove that the declarant thereafter acted in accordance with the stated intent").

[7] ECF No. 84-2 (Klein Decl.) at ¶¶ 21-34; ECF No. 89 (Marcus Decl.) at ¶¶ 56-58, 62, 72, 109.

[8] ECF No. 84-1 (Russell Decl.) at ¶¶ 5-6, 10-12, 15, 19-23.

[9] ECF No. 89 (Marcus Decl.) at ¶¶ 56-58, 62, 70-73, 77, 109, 128-47.

(*footnote continued on following page*)

The NSA Inspector General's draft report also is evidence of AT&T's participation in NSA's interception of Internet communications during the period from 2001 to 2007.[10]

Plaintiffs' declarations show that they are AT&T Internet customers who use the Internet to communicate internationally, including sending emails to persons located overseas and visiting foreign websites.[11]

The government has not submitted any evidence in the public record controverting any of plaintiffs' evidence. Instead, it contends that plaintiffs' evidence is insufficient to show that plaintiffs' communications ever have been or are currently being copied or searched by the government.

Plaintiffs' evidence described above (including the government's own admissions), however, establishes that since 2001 the government has been copying Internet communications transiting AT&T's Internet backbone network, filtering them in an attempt to eliminate wholly domestic communications, and searching them for selectors. As AT&T Internet customers who communicate internationally, plaintiffs' communications are among those copied, filtered, and searched.

(*footnote continued from preceding page*)
The Court overrules the government's objections to Marcus's testimony. Marcus's education and long experience with Internet businesses and technology, together with the facts stated in Klein's testimony and the AT&T documents (facts which are confirmed by Russell's testimony), give him a substantial foundation for his opinions.

[10] ECF No. 147, Ex. A (NSA Office of the Inspector General Report on the President's Surveillance Program, Working Draft ("NSA IG draft report")) at 17, 27-29, 33. The NSA IG draft report identifies "Company A" and "Company B" as participants in the NSA's Internet backbone surveillance and describes them as the two largest providers of international telephone calls into and out of the United States when the surveillance began in 2001. *Id*. AT&T was one of the two largest providers of international telephone calls in the United States at that time. ECF No. 262, Ex. E (Common Carrier Bureau, Federal Communications Commission, 1999 International Telecommunications Data) at 29, fig. 9.

[11] ECF No. 263 (Jewel Decl.) at ¶¶ 2-8; ECF No. 264 (Knutzen Decl.) at ¶¶ 2-9; ECF No. 265 (Walton Decl.) at ¶¶ 2-9.

Plaintiffs' evidence is sufficient to establish their standing. Standing is determined by the facts existing at the time the lawsuit was filed. *Davis v. Federal Election Commission*, 554 U.S. 724, 734 (2008). The cumulative evidence of the Klein, Russell, and Marcus declarations, the PCLOB report and other government admissions, the NSA IG draft report, and plaintiffs' own declarations shows that the copying and searching of the Internet communications of plaintiffs and other AT&T customers that began in 2001 was continuing in 2008 when this lawsuit was filed. The government defendants have not put forward any opposing evidence showing that their copying and searching of AT&T Internet backbone communications had ceased by 2008. Defendants' further suggestion that the copying and searching of communications transiting AT&T's Internet backbone may have ceased between 2008 and now also does not rise to the level of an evidentiary inference or create a genuine dispute of fact because it is not supported by any evidence, direct or circumstantial. To the contrary, the evidence shows that the government's Internet backbone surveillance, including full-content searching of the communications at stage three, is ongoing, and that AT&T continues to participate in FISA surveillance. Moreover, to the extent conduct by the government after the filing of this lawsuit might bear on the scope and appropriateness of injunctive relief, that issue is not presented by the pending motions.

C. Search And Seizure Of Plaintiffs' Communications

1. Seizure Of Internet Communications By "Stage One" Copying

The Fourth Amendment protects plaintiffs' email and other Internet communications, just as it protects communications in other forms. *United States v. Cotterman*, 709 F.3d 952, 957, 964-66 (9th Cir. 2013) (en banc) (emails and browsing history protected as "papers" under the Fourth Amendment); *Berger v. New York*, 388 U.S. 41, 59-60 (1967) (Fourth Amendment protects oral conversations); *Katz v. United States*, 389 U.S. 347, 353 (1967) (same); *Ex parte Jackson*, 96 U.S. 727, 733 (1877) (Fourth Amendment protects contents of letters while in transit); *see United States v. Jones*, 565 U.S. __, 132 S. Ct. 945, 950 (2012) (Fourth Amendment "embod[ies] a particular concern for government trespass upon the areas ('persons, houses, papers, and effects') it enumerates").

A seizure occurs when there is a meaningful interference with a possessory interest. *United States v. Jacobsen*, 406 U.S. 109, 113 (1984). An exercise of dominion and control by the government is one type of meaningful interference that results in a seizure. *Id*. at 120-21 & n.18. The parties agree, and the Court finds, that plaintiffs have a possessory interest in their Internet communications. Plaintiffs' possessory interest in the contents of their communications extends to the right to exclude others from copying their communications. *Hearst v. Black*, 87 F.2d 68, 70-71 (D.C. Cir. 1936) (government's copying of telegrams en masse was a "dragnet seizure" that violated sender's property right in contents of telegrams). Copying a communication in transit is a seizure because it is an exercise of dominion and control that meaningfully interferes with the possessory interest in the communication. *See Berger*, 388 U.S. at 59-60 (making an electronic copy of an oral conversation was a seizure of the conversation); *Katz*, 389 U.S. at 353 (same); *United States v. Ganias*, 755 F.3d 125, 137 (2d Cir. 2014) (copying of defendant's computer files beyond the scope of a warrant was a seizure since it "deprived him of exclusive control over those files"); *United States v. Jefferson*, 571 F. Supp. 2d 696, 701-704 (E.D. Va. 2008) (copying of personal information and documents is a seizure).

Accordingly, the Court holds that the "stage one" copying of plaintiffs' Internet communications is a seizure. It is an intrusion into plaintiffs' "papers" and an appropriation of their contents. The government argues that the copies exist only for "milliseconds" and therefore there is no seizure. This argument lacks both factual and legal foundation. There is no evidence in the record that the copies made last only milliseconds. Even if there were such evidence, it would not show that the making of the copies was not an exercise of dominion and control. The interference that plaintiffs complain of is the copying of the contents of their communications, not a delay in delivery of their communications. None of the package-delay cases that the government relies on involved opening the package to copy communications inside of it, and thus they do not support the government's position that copying the contents of a communication in transit is not a seizure so long as delivery of the communication is not delayed. However long the copies exist, it is long enough for the government to search their full contents and learn whether the communications contain any of the selectors the government is searching for.

2. "Stage Three" Search Of Internet Communications

A search occurs when the government violates a person's reasonable expectation of privacy or physically intrudes on a constitutionally protected area such as a person's papers to discover information. *Jones*, 132 S. Ct. at 949-50; *Florida v. Jardines*, __ U.S. __, 133 S. Ct. 1409, 1414 (2013). The parties agree, and the Court finds, that plaintiffs have a reasonable expectation of privacy in their Internet communications. *See Cotterman*, 709 F.3d at 964-66.

At stage three, the government searches the entire contents of plaintiffs' Internet communications for the selectors it is interested in. Searching the contents of a communication to determine whether or not it contains a particular message is an intrusion on the contents of the communication and violates the reasonable expectation of privacy in the communication. As such, it is a search for Fourth Amendment purposes.

The government argues that the full-content searching of plaintiffs' communications at stage three does not violate any reasonable expectation of privacy because no human ever learns of the result of the search. But even though the search is automated, the government learns whether or not the communication contains one or more selectors and uses that information to decide whether to retain the communication or not. The government discovers information about the contents of the communications and acts on that information. Moreover, despite the automated nature of the search, it is humans who have designed the search mechanism and who choose what selectors to search for.

The dog-sniff and other contraband detection cases that the government relies upon do not demonstrate that the content-searching of plaintiffs' communications is not a search. In those cases, the government without opening the package or container tried to detect an externally observable characteristic of contraband within. *Jacobsen*, 466 U.S. at 122-24; *United States v. Place*, 462 U.S. 696, 706-708 (1983) (holding dog sniffs are "*sui generis*"). Here, the government is going inside plaintiffs' communications and examining their contents, the equivalent of opening and searching a package en route. That conduct is a search. *Jacobsen*, 466 U.S. at 114 ("the Fourth Amendment requires that [the government] obtain a warrant before examining the contents of . . . a package").

D. Constitutionality Of The Search And Seizure

The seizures and searches of plaintiffs' Internet communications are made without a warrant or any individualized suspicion. Warrantless searches and seizures are presumptively unreasonable, as are suspicionless searches. *Jacobsen*, 466 U.S. at 114; *Chandler v. Miller*, 520 U.S. 305, 308 (1997). This is a consequence of the Fourth Amendment's purpose, which is to prevent suspicionless general searches and seizures. *Riley v. California*, 573 U.S. __, 134 S. Ct. 2473, 2494 (2014); *Payton v. New York*, 445 U.S. 573, 583 (1980); *Marcus v. Search Warrant of Property*, 367 U.S. 717, 726-29 & n.22 (1961); *Go-Bart Importing Co. v. U.S.*, 282 U.S. 344, 357 (1931).

The government contends that warrantless, suspicionless searches of plaintiffs' Internet communications are permitted here under the "special needs" exception. It contends that a significant purpose of the searches is to obtain foreign intelligence information and that this purpose justifies the intrusion on plaintiffs' possessory and privacy interests.

The "special needs" exception is a "closely guarded" category. *Chandler*, 520 U.S. at 309. It requires a "context-specific" inquiry. *Id*. at 314. A threshold requirement of the special needs exception is that "'the privacy interests implicated by the search [be] minimal.'" *Id*. (quoting *Skinner v. Railway Labor Executives' Ass'n*, 489 U.S. 602, 624 (1989)). Thus, circumstances in which the Supreme Court has approved warrantless special needs searches are ones in which the person searched has a diminished expectation of privacy, such as, for example, schoolchildren who voluntarily choose to participate in extracurricular activities, *see Board of Education of Independent School Dist. No. 92 of Pottawatomie County v. Earls*, 536 U.S. 822, 830-32 (2002); *Vernonia School Dist. 47J v. Acton*, 515 U.S. 646, 654-57 (1995), or workers who voluntarily choose employment in professions that put the safety of others at risk, *see Skinner*, 489 U.S. at 624-28; *National Treasury Employees Union v. Von Raab*, 489 U.S. 656, 671-72 (1989). As Justice Kennedy has explained: "An essential, distinguishing feature of the special needs cases is that the person searched has consented, though the usual voluntariness analysis is altered because adverse consequences (*e.g.*, dismissal from employment or disqualification from playing on a high

school sports team) will follow from refusal." *Ferguson v. City of Charleston*, 532 U.S. 67, 90-91 (2001) (Kennedy, J., concurring).

Here, plaintiffs' privacy interests in their Internet communications are within the Fourth Amendment's central protection of their "papers." Plaintiffs have an undiminished expectation of privacy in the content of their electronic communications and retain their possessory interest in their communications. They have not voluntarily chosen to engage in activities that diminish their expectations of privacy or otherwise consented to the search.

Nor is the intrusion into plaintiffs' privacy interest in their communications a minimal one. The intrusion into those communications is total: At stage one, the government copies the contents of all of plaintiffs' communications flowing through AT&T's Internet backbone junctions. For those communications that pass through the filtering at stage two and are searched at stage three, the entire contents are searched.

The undiminished nature of plaintiffs' privacy interests in their Internet communications also makes the seizures and searches unreasonable under the Fourth Amendment. "The cases in which the [Supreme] Court has found warrantless searches to be reasonable all involve . . . greatly diminished privacy interests—a point repeatedly emphasized by the Court." *Al Haramain Islamic Foundation, Inc. v. United States Department of Treasury*, 686 F.3d 965, 994 (9th Cir. 2011). As explained, plaintiffs' privacy interests are undiminished, making the searches and seizures unreasonable.

E. The State Secrets Privilege

The government defendants also assert that the state secrets privilege requires dismissal of plaintiffs' Fourth Amendment claim alleging ongoing Internet surveillance. The government does not assert that any of the evidence on which plaintiffs rely is privileged. Indeed, it has affirmatively waived any privilege as to the evidence of AT&T's participation in the surveillance set forth in the Klein and Marcus declarations and the AT&T documents. ECF No. 295, Ex. C.

Instead, it contends that secret evidence exists that precludes a "full and fair adjudication" of plaintiffs' claim.[12] ECF No. 285 at 45.

The Court rejects the government's contention that the state secrets privilege requires dismissal of plaintiffs' Fourth Amendment claim alleging ongoing Internet surveillance. In earlier proceedings, the Court ruled that Congress has displaced the state secrets privilege for plaintiffs' statutory claims of unlawful electronic surveillance with the procedure of 50 U.S.C. § 1806(f). *Jewel*, 965 F. Supp. 2d at 1103-1106. The parties agree and the Court concludes that its analysis applies equally to plaintiffs' constitutional claims, and the Court accordingly holds that section 1806(f) displaces the state secrets privilege in the adjudication of plaintiffs' constitutional claims. *See* ECF No. 167 at 2, 6-7.

Under section 1806(f), Congress has charged the courts with deciding claims of unlawful electronic surveillance on their merits, rather than dismissing such claims. *Jewel*, 965 F. Supp. 2d at 1104-1105. "The purpose of this provision is to permit courts to determine whether any particular surveillance was lawfully authorized and executed." *Id*. at 1105. Any secret evidence necessary for adjudicating the constitutionality of the government's mass surveillance can be submitted to the Court for its *in camera* and *ex parte* consideration in deciding the lawfulness of the surveillance. *Id*. at 1104-1105. The government, however, has not sought to proceed by way of section 1806(f). Instead, it continues to maintain its position that section 1806(f) does not displace the state secrets privilege or apply to any of plaintiffs' claims, and that the Court should not consider any secret evidence in adjudicating the merits of plaintiffs' motion. 12/19/14 RT at 42-45, 47, 119. In light of that choice by the government and the government's position that any secret evidence must be excluded from the process of deciding the merits of plaintiffs' motion, it is

[12] The government cites no authority for its contention that the state secrets privilege requires dismissal whenever the exclusion of evidence makes an adjudication less "full and fair" than it would otherwise be, and that contention is inconsistent with the nature of the state secrets privilege as an evidentiary privilege. Invocation of a privilege always results in the exclusion of relevant evidence and in that sense makes the resulting adjudication less "full and fair" than it would be if the evidence were admitted.

appropriate for the Court to decide the merits of plaintiffs' motion using only the public evidence of record.

Finally, the Court rejects the government's position that any ruling on plaintiffs' claim would inevitably harm national security. AT&T's participation in Internet surveillance for national security purposes is public knowledge by virtue of the Klein evidence and AT&T's admissions. And as this order demonstrates, a ruling on plaintiffs' claim does not disclose the identities of those "on the list of surveillance targets." *Clapper v. Amnesty International USA*, __ U.S. __, 133 S. Ct. 1138, 1149 n.4 (2013).

CONCLUSION

For the foregoing reasons, the Court GRANTS plaintiffs' motion for partial summary judgment and DENIES the government defendants' cross-motion for partial summary judgment. The Court holds that the government defendants' warrantless and suspicionless seizure of plaintiffs' Internet communications violates the Fourth Amendment, and that the government defendants' warrantless and suspicionless content-searching of plaintiffs' Internet communications violates the Fourth Amendment.

IT IS SO ORDERED.

Dated: _____

_____
JEFFREY S. WHITE
UNITED STATES DISTRICT JUDGE