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

PLAINTIFFS CAROLYN JEWEL, ERIK KNUTZEN, AND JOICE WALTON'S COMBINED REPLY IN SUPPORT OF THEIR MOTION FOR PARTIAL SUMMARY JUDGMENT AND OPPOSITION TO THE GOVERNMENT DEFENDANT'S CROSS-MOTION FOR PARTIAL SUMMARY JUDGMENT

(Fourth Amendment Violation)

Date: December 19, 2014
Time: 9:00 a.m.
Courtroom 5, Second Floor
The Honorable Jeffrey S. White

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Federal Cases

State Cases

Federal Statutes

Federal Rules

Constitutional Provisions

Legislative Materials

Other Authorities

INTRODUCTION

The government does not contest the fundamental Fourth Amendment principles set forth in plaintiffs' motion—that Americans deserve to be secure in their papers and effects and that the Constitution grants them that security, chiefly, by ensuring that a judge issues a particularized warrant upon probable cause prior to a search or seizure. These principles played a fundamental role in the founding of this country and have been zealously guarded by the courts ever since.

The government instead contends that those principles have no application here, where the government is unequivocally breaching the security and privacy of the papers and effects of millions of individuals. Its position essentially is that it can circumvent the Fourth Amendment's core principles by copying communications in transit on the Internet instead of taking physical possession of the originals, and by searching their contents very quickly with computers instead of searching them with humans. The government further contends that if one of its purposes for the copying and searching the communications is foreign intelligence, then the circumvention is complete, and the Internet has for all practical purposes become a Fourth-Amendment-free zone.

The government is wrong. The wholesale, dragnet copying of innocent communications is a seizure; the subsequent full-text review of the content of hundreds of millions of those communications is a search. With a scale reaching the Internet activities of millions of innocent Americans, the foreign intelligence purpose the government articulates is simply insufficient to create an exception to the warrant requirement or to make its seizures and searches reasonable.

Plaintiffs are entitled to summary judgment.

ARGUMENT

I. The Government's Mass Interception And Copying Of The Internet Communications Of Plaintiffs And Millions Of Other Americans Is A Seizure

A. The Fourth Amendment Protects Plaintiffs' Possessory Interest In The Exclusive Dominion and Control Of The Content Of Their Internet Communications

The Fourth Amendment protects "papers" and "effects" not merely for their status as objects, but also for the information they contain. *See Ex parte Jackson*, 96 U.S. 727, 733 (1877) (protection of letter's contents in transit). As explained in plaintiffs' Motion for Partial Summary Judgment

(ECF No. 261; hereinafter "plaintiffs' motion"), the Fourth Amendment's protection of "papers" and "effects" applies to the contents of digital communications in transit and prohibits their warrantless seizure by copying. *See* Plaintiffs' Motion (ECF No. 261) at 11-12. As the Seventh Circuit observed when holding that IRS agents had engaged in a seizure merely by taking notes and taping dictation describing the contents of certain documents, it "is the information and not the paper and ink itself" that is actually seized. *LeClair v. Hart*, 800 F.2d 692, 696 n.5 (7th Cir. 1986).

A seizure occurs when "there is some meaningful interference with an individual's possessory interests" in property. *U.S. v. Jacobsen*, 466 U.S. 109, 113 (1984). "'[A] possessory interest derives from rights in property delineated by the parameters of law.'" *U.S. v. Jefferson*, 566 F.3d 928, 934 (9th Cir. 2009). As the Ninth Circuit has confirmed, "[a] 'possessory or ownership interest' need not be defined narrowly." *U.S. v. Thomas*, 447 F.3d 1191, 1197-99 (9th Cir. 2006) (unauthorized driver of a rental car had possessory interest in the car). Here, plaintiffs have a possessory interest in the contents of their communications and that interest extends to the right to exclude others from copying their communications. Plaintiffs' possessory interest in the contents of their communications exists under property law—including copyright and the common law (*see* 17 U.S.C. § 106; *Carpenter v. U.S.*, 484 U.S. 19, 26 (1987) ("Confidential business information has long been recognized as property.")—and under tort law, which protects against the invasion and misappropriation of private information (*see Shulman v. Group W Prods., Inc.*, 18 Cal. 4th 200, 232 (1998) (tort to "obtain[] unwanted access to data about[] the plaintiff").

An exercise of "dominion and control" by the government is one type of meaningful interference that results in a seizure. *Jacobsen*, 466 U.S. at 120-21 & n.18. It can occur when the government asserts control over an item entrusted to a service provider for transit. *Id*. As the *Jacobsen* court noted: "[T]he agents took custody of the package from Federal Express after they arrived. Although respondents had entrusted possession of the items to Federal Express, the decision by governmental authorities to exert dominion and control over the package for their own purposes clearly constituted a 'seizure,' . . . ." *Id*. (citing *U.S. v. Van Leeuwen*, 397 U. S. 249 (1970)).

The government interferes with plaintiffs' possessory interests in their communications and exercises dominion and control over them when it copies those communications at stage one, even though the communications are in transit in intangible form.[1] "[W]hile copying the contents of a person's documents by way of photographs or written notes does not interfere with a person's possession of those documents, it does interfere with the person's sole possession of the information contained in those documents: it diminishes the person's privacy value in that information." *U.S. v. Jefferson*, 571 F. Supp. 2d 696, 703 (E.D. Va. 2008). This is because "the Fourth Amendment protects an individual's possessory interest in information itself, and not simply in the medium in which it exists." *Id*. at 702; *see also In re Search of Info. Associated with [Redacted] at mac.com*, No. 14–228 (JMF), 2014 WL 1377793, at *3 (D.D.C. Apr. 7, 2014) (collecting cases in which copying e-mails held a seizure), *vacated on other grounds*, 2014 WL 4094565 (D.D.C. Aug. 8, 2014).

Indeed, the Supreme Court has long held that intangible communications are seized when they are copied. In *Berger v. New York*, the Court found an electronic eavesdropping statute unconstitutional because it lacked any requirement of particularity and gave officers "a roving commission to 'seize' any and all conversations." 388 U.S. 41, 59 (1967). Noting that the "property sought" was intangible conversations, the Court repeatedly referred to the act of recording—that is, copying—the conversation as a "seizure" under the Fourth Amendment. *Id.* at 59-60. Similarly, in *Katz v. U.S.*, the Court held that "electronically listening to and *recording* the petitioner's words . . . constituted a 'search and seizure' within the meaning of the Fourth Amendment." 389 U.S. 347, 353 (1967) (italics added); *accord Hoffa v. U.S.*, 385 U.S. 293, 301 (1966) ("the protections of the Fourth Amendment are surely not limited to tangibles, but can extend as well to oral statements"); *Caldarola v. Cnty. of Westchester*, 343 F.3d 570, 574 (2d Cir. 2003) (videotaping suspect was a seizure of his image; "The Fourth Amendment seizure has long encompassed the seizure of intangibles as well as tangibles.").

[1] Stage one is described in Plaintiffs' Motion (ECF No. 261) at 5-6.

Thus, the government may interfere with intangible possessory interests in information just as it does with physical property—by depriving a person of "exclusive control" over the information. *U.S. v. Ganias*, 755 F.3d 125, 137 (2d Cir. 2014). In *Ganias*, the Second Circuit had no difficulty finding that the act of copying of a defendant's computer files beyond the scope of a warrant was a seizure since it "deprived him of exclusive control over those files." *Id*. at 137. In *U.S. v. Comprehensive Drug Testing, Inc.*, the Ninth Circuit likewise held that the government had improperly "seized" data when it copied electronic data outside the scope of a search warrant.[2] 621 F.3d 1162, 1166 (9th Cir. 2010) (en banc); *id*. at 1176 ("Seizure of, for example, Google's email servers to look for a few incriminating messages could jeopardize the privacy of millions.").

Making a copy of plaintiffs' electronic data, as the government does here, interferes with their right to control the information contained in the original copy and is thus a seizure.[3] *Ganias*, 755 F.3d at 137; *Jefferson*, 571 F. Supp. 2d at 702-03; Orin S. Kerr, *Fourth Amendment Seizures of Computer Data*, 119 Yale L.J. 700, 707 (2010). The government exercises "dominion and control" over the communications by making copies of them with the splitter at stage one and subsequently filtering and then searching the copies at stages two and three. *See Jacobsen*, 466 U.S. at 120-21; Plaintiffs' Motion (ECF No. 261) at 4-8. Because plaintiffs have a possessory interest in their communications, the act of copying is a substantial interference with that interest. By making a complete unauthorized copy of plaintiffs' communications, the government seizes the communications and usurps plaintiffs' dominion and control over the information in those communications. *Id*.

---

[2] Before *Comprehensive Drug Testing,* two district courts in the Ninth Circuit had reached the opposite conclusion. *U.S. v. Gorshkov,* No. CR00-550C, 2001 WL 1024026, at *3 (W.D. Wash. May 23, 2001); *In re Application of the U.S. for a Search Warrant for Contents of Electronic Mail*, 665 F. Supp. 2d 1210, 1222 (D. Or. 2009). These decisions are no longer sound authority.

[3] Whether the seizures and searches here are conducted by the government or by AT&T at the government's direction is irrelevant. The Fourth Amendment applies whenever a "private party acts as an 'instrument or agent' of the government." *U.S. v. Young*, 153 F.3d 1079, 1080 (9th Cir. 1998); *accord U.S. v. Davis*, 482 F.2d 893, 897 (9th Cir. 1973) (search of airline passengers by airline employees at government's direction was a government search; "The Fourth Amendment applies to a search whenever the government participates in any significant way in th[e] total course of conduct."), *overruled on other grounds by U.S. v. Aukai*, 497 F.3d 955 (9th Cir. 2007).

Thus, contrary to the government's assertion, plaintiffs do have a possessory interest in the contents of their communications even when their communications are in the form of "modulated electromagnetic impulses moving . . . across fiber-optic networks." Govt. Opp. (ECF No. 285) at 26. Under the government's argument, digital information would never be considered "seized" unless the government took possession of some sort of physical artifact like a hard drive or a server. But the scope of the Fourth Amendment's protections do not vary depending on whether a person's information is carried by ink written on tree pulp or by light waves. *See Berger*, 388 U.S. at 59-60 (conversation was seized when recorded). And of course it is plaintiffs' information, not the light waves that carry it, that the government seeks here.

The conclusion that a seizure is effected the moment plaintiffs' communications are copied is consistent with the Wiretap Act's prohibition against "intercept[ing] any wire, oral, or electronic communication," 18 U.S.C § 2511(1)(a), "through the use of any electronic, mechanical, or other device," *id*. at § 2510(4). The Wiretap Act is instructive because Congress drew many of its provisions "to meet the constitutional requirements for electronic surveillance enunciated by" the Supreme Court in *Berger* and *Katz*. *United States v. U.S. Dist. Ct.* (*Keith*), 407 U.S. 297, 302 (1972). As discussed above, *Berger* and *Katz* speak directly to the Fourth Amendment's protection against seizure of intangible communications. Under the Wiretap Act, interception occurs the moment communications are captured by a device, not when the copy is later listened to by a human. *U.S. v. Turk,* 526 F.2d 654, 658 (5th Cir. 1976); *Jacobson v. Rose*, 592 F.2d 515, 522 (9th Cir. 1978) (act of listening is unnecessary to establish interception). As the Ninth Circuit has explained, interception "occurs 'when the contents of a wire communication are captured or redirected in any way.'" *Noel v. Hall*, 568 F.3d 743, 749 (9th Cir. 2009). The First Circuit has likewise held that emails are intercepted when they are diverted while in transit in order to be copied. *U.S. v. Councilman*, 418 F.3d 67, 70-71, 79 (1st Cir. 2005) (en banc). Here, the government intercepts and seizes plaintiffs' communications by copying and diverting them through the splitter at stage one, regardless of whether they are later retained after stages two and three.

B. The Fourth Amendment Protects Communications in Transit; The Government's Arguments To The Contrary Must Be Rejected

1. Even Short-Lived Copies Interfere With Plaintiffs' Possessory Interest And Constitute A Seizure

The government raises a straw man by arguing that whether a seizure occurs here depends on whether it has delayed delivery of plaintiffs' Internet communications. Plaintiffs do not contend that the seizure takes the form of a delay in their communications; rather, the copying is itself the seizure, irrespective of any delay.[4] Because the government seizes plaintiffs' communications the moment it creates a copy, the length of time the government keeps these copies is irrelevant to the question of whether a seizure has occurred. In any event, even a "brief detention[]" of a person's luggage for a dog-sniff is a "seizure."[5] *U.S. v. Place*, 462 U.S. 696, 697-99, 702-03, 706-07 (1983).

2. The Government's Reliance On Contraband Cases In Which Packages Are Externally Inspected Is Misplaced

The government's reliance on cases in which a sealed package or luggage in transit was lifted, dog-sniffed, or otherwise had its external physical characteristics briefly inspected for signs of contraband without the package or luggage being opened is misplaced. Govt. Opp. (ECF No. 285) at 26-27. The question here is whether the wholesale copying of the contents of millions of communications for the purpose of content searching constitutes a seizure, but the government's authorities address only the detention of a single object in transit to conduct a brief external physical examination aimed solely at detecting contraband. None of the government's cases bears any resemblance to the seizures here: none involves the wholesale copying of communications and then, for millions of the seized communications, top-to-bottom full-text searching. The possessory

---

[4] The government repeatedly and erroneously asserts that plaintiffs' position is that the government maintains possession of the copies for only "milliseconds." Govt. Opp. (ECF No. 285) at 28. Plaintiffs make no contention about how long the government maintains possession of the copies, for it is the copying that is the seizure, regardless of how long the government retains the copies.

[5] Moreover, where, as here, the purpose of a seizure is a subsequent search that requires probable cause, the seizure also requires probable cause. This is true "no matter how brief" the seizure is. As the Supreme Court observed in *Place*: "The purpose for which respondent's luggage was seized, of course, was to arrange its exposure to a narcotics detection dog. Obviously, if this investigative procedure is itself a search requiring probable cause, the initial seizure of respondent's luggage for the purpose of subjecting it to the sniff test—*no matter how brief*—could not be justified on less than probable cause." 462 U.S. at 706 (italics added).

interests at issue in the two situations—the interest in a package or luggage continuing on its journey versus the interest in excluding others from copying one's communications and other data—have nothing in common. *Ex parte Jackson*, 96 U.S. at 733. Moreover, the transience of the detention in the contraband cases meant that the government received only a limited amount and type of information from its external examination. Here, however, even if the government copies the contents of all the communications it intercepts and completes its filtering and full-text analysis in a blink of an eye, the duration of the seizure bears no relationship to its intrusiveness.

The government's cases simply do not speak to either the possessory interest in the contents of a communication, or the interference with that possessory interest that occurs when the communication is copied. None involved inspecting or copying communications or other data found inside a package or luggage. In *U.S. v. Hoang*, for example, an external dog-sniff occurred without any detention or diversion of the package at all; the dog was let loose in a parcel processing room at Federal Express. 486 F.3d 1156, 1158 (9th Cir. 2007). Only after the dog alerted on the package and the police had reasonable suspicion that the package contained contraband did they detain the package, and the package was not opened until a warrant was obtained. *Id*. The other package and luggage cases also did not involve copying data or communications inside the container. *See U.S. v. England*, 971 F.2d 419, 420 (9th Cir. 1992) (dog-sniff of package in the mails); *U.S. v. Va Lerie*, 424 F.3d 694, 696-97 (8th Cir. 2005) (en banc) (moving luggage from bus to bus station where passenger was located to ask passenger's consent to search); *U.S. v. Brown*, 884 F.2d 1309, 1311 (9th Cir. 1989) (similar); *U.S. v. Hall*, 978 F.2d 616, 618 (10th Cir. 1992) (lifting luggage to check its weight); *U.S. v. Schofield,* 80 Fed. Appx. 798, 803 (3d Cir. 2003) (nonprecedential opinion; lifting detergent box to reveal only its unusual weight "almost certainly" not a seizure); *U.S. v. DeMoss*, 279 F.3d 632, 634-35 (8th Cir. 2002) (lifting package off conveyer belt not a seizure because officers observed only external details that the sender had "virtually guaranteed . . . could be observed by the senses"), *U.S. v. Gant,* 112 F.3d 239, 242 (6th Cir. 1997) (removing bag from overhead compartment revealed nothing); *U.S. v. Harvey*, 961 F.2d 1361, 1363 (8th Cir. 1992) (same).

The government wildly overreads the Ninth Circuit's statement in *U.S. v. Jefferson* that the possessory interest in a package is "solely in the package's timely delivery." 566 F.3d at 933. The Ninth Circuit was speaking only of the detention of a physical container for an external inspection, not authorizing the copying of information or communications transported within the container. Under the government's expansive and unsupported reading of *Jefferson*, it could open and copy every single letter mailed in the United States, and there would be no seizure of those communications so long as the original letters were put back in their envelopes and delivered on time. The government likewise overreads *Arizona v. Hicks*, a case holding that recording a serial number on the outside of a stolen stereo component was not a seizure of the number. 480 U.S. 321, 324 (1987). The serial number on the stolen component was not a writing or information the defendant had created and was not part of the defendant's "papers," unlike plaintiffs' communications. Like an odor detected by a dog sniff, the serial number was an externally observable characteristic that was used to determine whether the component was contraband.[6]

As explained in plaintiffs' motion, an unbounded seizure for "detailed examination of records not described in a warrant" is repugnant to the Fourth Amendment. *U.S. v. Tamura*, 694 F.2d 591, 595 (9th Cir. 1982); Plaintiffs' Motion (ECF No. 261) at 17. The fact that the government can thereafter search the entire scope of the information seized quickly due to modern computer processing power does not eliminate the fact of the initial seizure. The parallels between the general warrants of colonial times that allowed the papers of innocent people to be seized and the general seizures occurring here are clear and obvious. The unifying aspect is the untargeted nature of the authority claimed. While the "papers" that in colonial times were located in the home now

[6] The government erroneously asserts that *Hicks* held that moving the component to view the number was not a seizure. Govt. Opp. (ECF No. 285) at 27. The Supreme Court did not address this point, holding only that "the mere recording of the serial numbers did not constitute a seizure." *Hicks*, 480 U.S. at 324. It held that moving the component to view the number was an unconstitutional search. *Id*.

regularly travel over the Internet, a person's possessory interest in the content of those "papers" is no less substantial today than it was in the eighteenth century.[7]

II. The Government's Examination Of The Contents Of Plaintiffs' Internet Communications Is A Search

"A 'search' occurs when an expectation of privacy that society is prepared to consider reasonable is infringed." *Jacobsen*, 466 U.S. at 113. As set forth in plaintiffs' motion, the government conduct a search when, on an ongoing basis and without any modicum of suspicion, it subjects plaintiffs' Internet activity to "electronic scanning" in the hopes of finding "selectors" that might reveal communications with suspected terrorists.

The government's contention that it has not searched plaintiffs' Internet communications must be rejected. The government concedes that plaintiffs have a reasonable expectation of privacy in their Internet communications. However, it contends that its dragnet surveillance of those communications does not *compromise* that interest, and thus is not a search at all, because the communications without the selectors are never "provided to Government officials" or seen by human eyes. Govt. Opp. (ECF No. 285) at 31.

The government's human-eyes thesis is both incorrect and unsupported by authority. No case has drawn the line between searches and non-searches on the basis of exposure to human eyes. And, indeed, were the government's approach deemed to be the law, it would effectively authorize a digital surveillance state in which a person's every action and interaction could be technologically monitored and subject to electronic analysis without violating the Fourth Amendment, as long as all

[7] Contrary to the government's assertion (Govt. Opp. (ECF No. 285) at 30 n.6), Congress found that the NSA violated the Fourth Amendment in Operation Shamrock when it initially made copies of millions of international telegrams, not just by later reading a much smaller subset of them. S. Select Comm. to Study Governmental Operations with Respect to Intelligence Activities, *Book II: Intelligence Activities and the Rights of Americans*, S. Rep. No. 94-755 at 6, 12, 139 (1976), *available at* http://www.intelligence.senate.gov/pdfs94th/94755_II.pdf. Likewise in *Hepting*, the Court recognized that the initial acquisition of these same plaintiffs' communications by the dragnet here was a constitutional violation. *Hepting v. AT&T Corp.*, 439 F. Supp. 2d 974, 1009-10 (N.D. Cal. 2006) ("Plaintiffs' constitutional claim alleges that AT&T provides the government with direct and indiscriminate access to the domestic communications of AT&T customers. . . . AT&T's alleged actions here violate the constitutional rights clearly established in *Keith*.").

any human saw was "suspicious" information selected by the technology that some human had programmed.[8] The Fourth Amendment provides greater liberty than that.[9]

To support this argument, the government attempts to extend the holding of *Place*, 462 U.S. at 707, which the Supreme Court held was "*sui generis*," far beyond its facts. In *Place*, the Court held that a "canine sniff" of a single piece of luggage did not constitute a search, relying on two factors. First, the Court noted that a canine sniff "does not require opening the luggage" or an "officer's rummaging through the contents of the luggage." *Id*. Second, the Court noted that "the sniff discloses only the presence or absence of narcotics, a contraband item." *Id.* The Court stated, "[w]e are aware of no other investigative procedure that is so limited both in the manner in which the information is obtained and in the content of the information revealed[.]" *Id*.

It is this second characteristic of *Place*, the fact that the search was designed to detect *only* contraband and nothing else, that has been subsequently recognized as the critical factor. *See Illinois v. Caballes*, 543 U.S. 405, 409 (2005) ("[W]e treated a canine sniff by a well-trained narcotics-detection dog as '*sui generis*' because it 'discloses only the presence or absence of narcotics, a contraband item.'"). Indeed, the Court has declined to apply *Place* when the non-human technology used was "capable of detecting lawful activity." *Id*.

The government's only other authority has been confined to its facts on the very same basis. In *Jacobsen*, the Supreme Court applied *Place* to find that no search was conducted when a chemical test was performed on a white powder found leaking out of package. 466 U.S. at 123. The Court held that "governmental conduct that can reveal whether a substance is cocaine, and no other

---

[8] *See City of Indianapolis v. Edmond*, 531 U.S. 32, 42 (2000) (cautioning that applying "a high level of generality" to Fourth Amendment search questions would provide "little check on the ability of authorities").

[9] "We cannot accept the Government's contention that it should be completely free from the constraints of the Fourth Amendment to determine by means of an electronic device, without a warrant and without probable cause or reasonable suspicion, whether a particular article—or a person, for that matter—is in an individual's home at a particular time. Indiscriminate monitoring of property that has been withdrawn from public view would present far too serious a threat to privacy interests in the home to escape entirely some sort of Fourth Amendment oversight." *U.S. v. Karo*, 468 U.S. 705, 716 (1984).

arguably 'private' fact, compromises no legitimate privacy interest." *Id*. The Court explicitly stated that its discussion was "confined to possession of contraband." *Id.* at 123 n.23.

Thus in each case, it was not the fact that the investigation was performed by a non-human that rendered it a non-search, but the fact that any expectation of privacy in hiding contraband, when the contraband was the only thing capable of being detected by the search, is simply not "an interest in 'privacy that society is prepared to consider reasonable.'" *Caballes*, 543 U.S. at 409 (quoting *Jacobsen*, 466 U.S. at 122). "We have held that any interest in possessing contraband cannot be deemed 'legitimate,' and thus, governmental conduct that *only* reveals the possession of contraband 'compromises no legitimate privacy interest.'" *Id*. at 408-09 (italics original); *see also U.S. v. Young*, 573 F.3d 711, 720–21 (9th Cir. 2009) (declining to extend *Jacobsen* to search of backpack that did not contain only contraband).

When the investigative technique is not limited to the detection of contraband, *Place* and *Jacobsen* have no application. "The legitimate expectation that information about perfectly lawful activity will remain private is categorically distinguishable from respondent's hopes or expectations concerning the nondetection of contraband in the trunk of his car." *Caballes*, 543 U.S. at 410.

Indeed, *Place* cannot even be extended to all dog sniffs. In *Edmond*, 531 U.S. at 40, 44, the Court invalidated the use of a narcotics-sniffing dog at a vehicle checkpoint because, like here, it was used as part of a program of mass suspicionless seizures. And in *Florida v. Jardines,* __ U.S. __, 133 S. Ct. 1409, 1413, 1417-18 (2013), the Supreme Court found it was a search to use a drug-sniffing dog on a homeowner's porch to investigate the contents of the home.

The government does not and cannot claim that the items identified by the search here, Internet communications identified by the selectors, are "contraband." Moreover, unlike narcotics dogs—which are trained to detect particular odor molecules emanating from physical objects—or a chemical drug test—which is scientifically designed to react to particular chemical compounds—stage three of the government's surveillance searches the entire contents of the communications. Stage three thus discloses the answer to a multitude of questions—not a single, specific question—and the program can be modified to answer different, or more, questions at any time. Indeed, choosing the search terms employed in stage three of the government's surveillance involves an

exercise of discretion that simply does not exist when teaching a dog to detect cocaine or developing a chemical test to react to particular narcotics.[10]

Rather, the government's searching of communications here is more analogous to the use of a "hash value" scan of a computer hard drive, which has been held to be a search. A hash value is an alphanumeric value unique to each computer file that can be used to confirm whether two digital files are the same. FEDERAL JUDICIAL CENTER, MANAGING DISCOVERY OF ELECTRONIC INFORMATION: A POCKET GUIDE FOR JUDGES 38 (2d ed. 2012). In *U.S. v. Crist*, 627 F. Supp. 2d 575, 578, 585 (M.D. Pa. 2008) the court held that "the 'running of hash values' is a search protected by the Fourth Amendment." 627 F. Supp. 2d 575, 578, 585 (M.D. Pa. 2008). "By subjecting the entire computer to a hash value analysis—every file, internet history, picture, and 'buddy list' became available for Government review." *Id.* at 585. "Such examination constitutes a search." *Id.*

An analogy even closer to the mass surveillance here is found in *Bourgeois v. Peters*, in which a city requirement that every one of the 15,000 people who sought to attend an annual protest outside of a military base pass through a magnetometer was found to be an unconstitutional search. 387 F.3d 1303, 1307, 1316 (11th Cir. 2004). A magnetometer only detects the presence of metal, providing no other information to the human monitoring it. *Id.* at 1307 n.2. And it neither retains nor tells the person monitoring it anything about anyone who does not possess metal. The court rejected the city's argument that the magnetometric screening was justified by both past incidents of violence at previous editions of the protest and the "elevated" terrorist threat status issued by the Department of Homeland Security. *Id.* at 1310-12. Emphasizing the complete absence of any legal

[10] The government's "selectors" are nothing like a dog-sniff or chemical test that gives the searcher no discretion as to what is being searched for. Section 702 leaves not only the selection of targets to the discretion of NSA personnel, but also leaves the choice of search selectors for each target to the NSA's discretion without any FISC review—selectors that the NSA uses to search all communications in stage three. *See* Plaintiffs' Motion (ECF No. 261) at 21-23. Because section 702 broadly defines "foreign intelligence information," targets and selectors need not be associated with any nefarious activity. 50 U.S.C. §§ 1801(e), 1881a(g)(2)(A)(v). It also leaves to the NSA the discretion to choose the number of selectors per target, along with the discretion to change its list of selectors and add new ones. *See* Plaintiffs' Motion (ECF No. 261) at 21-23. In principle and practice, the NSA, not a judge, decides what it will search plaintiffs' communications for, making the section 702 process a general warrant. *See id*.

support for "the broad authority to conduct mass, suspicionless, warrantless searches," the court explained that the city's position "would effectively eviscerate the Fourth Amendment." *Id.* at 1311. To the contrary, the Fourth Amendment "establishes searches based on evidence—rather than potentially effective, broad, prophylactic dragnets—as the constitutional norm." *Id.* at 1312; *see Lebron v. Wilkins*, 820 F. Supp. 2d 1273, 1283 (M.D. Fla. 2011) (finding a Fourth Amendment search where drug testing of all welfare recipients was required to receive benefits, but only positive results were stored in a database accessible to government officials).

Yet, although they are closer than the examples offered by the government, neither *Crist* (which involved the scan of a single computer) nor *Bourgeois* (in which the suspicion was based on past incidents of illegal activity) fully reflects the scope of the surveillance or the complete lack of suspicion in the present case. The mass suspicionless surveillance of plaintiffs', and millions of other Americans', Internet communications is far broader in scope than the limited, no-human-eyes contraband investigations that have been found not to be searches. Internet backbone surveillance does not simply subject a single car or a single suitcase to review. It is exponentially greater than the 15,000 people subjected to mass surveillance on a single day in *Bourgeois*. Instead, millions of people have hundreds of millions of their communications reviewed, and the surveillance is continuous. The expansion is thus twofold – both the number of nonsuspect people subject to the review and the number of nonsuspect communications reviewed is grossly greater than any that have been or could be subject to dog sniffs or chemical testing in the precedents the government relies upon. Investigatory methods, even if undertaken for a legitimate law enforcement purpose, and even if employing a non-human investigative technique, must be proportionate and carefully focused. *See Edmond*, 531 U.S. at 42-45.

III. The Intrusive Searches And Seizures Here Are Outside The Scope Of Any "Foreign Intelligence" Or Other "Special Needs" Exception To The Warrant Requirement

A. No "Special Needs" Exception Exists On These Facts

The warrant requirement applies to the government's mass suspicionless seizures and searches here. As plaintiffs' motion explains, the Fourth Amendment protects plaintiffs' "papers" and "effects" from being seized and searched without a warrant. The Fourth Amendment has always

provided heightened protection for the contents of communications like the Internet communications at issue here.

As plaintiffs' motion also explains, the Supreme Court has recognized only "'a few specifically established and well-delineated exceptions'" to the warrant requirement. *Al Haramain Islamic Foundation, Inc. v. U.S. Department of Treasury*, 686 F.3d 965, 990 (9th Cir. 2011) (quoting *Katz*, 389 U.S. at 357); *see* Plaintiffs' Motion (ECF No. 261) at 24-25. One of these is the "closely guarded" "special needs" exception. *Chandler v. Miller*, 520 U.S. 305, 309 (1997).

The government contends that the special needs exception authorizes the searches and seizures here because a significant purpose of the surveillance is to gather information about foreign powers and their agents. Govt. Opp. (ECF No. 285) at 36-37. But those lower courts that have applied the special needs exception to foreign intelligence gathering have done so with respect to activities far different—and far more targeted—than the mass suspicionless surveillance at issue here. The Supreme Court has never endorsed the application of the special needs exception to foreign intelligence gathering, much less extended it to authorize the seizure and searching of the communications of innocent Americans not suspected of being agents of foreign powers. *See Keith*, 407 U.S. at 321-22. Indeed, Justice Scalia, writing for a unanimous panel of the D.C. Circuit, held that the warrant "requirement attaches to national security wiretaps that are not directed against foreign powers or suspected agents of foreign powers." *Halperin v. Kissinger*, 807 F.2d 180, 185 (D.C. Cir. 1986). That rule governs here, because plaintiffs are not agents of foreign powers and yet the government is intentionally seizing and searching their communications, along with those of millions of other Americans.

An analysis under the special needs doctrine confirms that the warrant requirement applies here. As the high court has emphasized, "[w]hen such 'special needs'—concerns other than crime detection—are alleged in justification of a Fourth Amendment intrusion, courts must undertake a *context-specific inquiry*, examining closely the competing private and public interests advanced by the parties." *Chandler*, 520 U.S. at 314 (italics added); *accord Ferguson v. City of Charleston*, 532 U.S. 67, 78 (2001).

Under the context-specific special needs inquiry, "'[i]n limited circumstances, where the privacy interests implicated by the search are minimal, and where an important governmental interest furthered by the intrusion would be placed in jeopardy by a requirement of individualized suspicion, a search may be reasonable despite the absence of such suspicion.'" *Chandler*, 520 U.S. at 314; *accord Ferguson*, 532 U.S. at 78 ("a balancing test that weighed the intrusion on the individual's interest in privacy against the 'special needs' that supported the program").

Further, the government must show that the primary purpose of the intrusion is something other than law enforcement. *Edmond*, 531 U.S. at 40-48. "[T]o determine the relevant primary purpose," the court must "consider all the available evidence." *Ferguson*, 532 U.S. at 81; *accord Edmond*, 531 U.S. at 46. Finally, the government must show in addition that complying with the warrant requirement would be impracticable. *Skinner v. Ry. Labor Executives' Ass'n*, 489 U.S. 602, 631 (1989).

As plaintiffs' motion explains, the suspicionless mass search and seizure of Americans' Internet communications fails the first prong of the "special needs" exception, which requires that "the privacy interests implicated by the search [be] minimal." *Chandler*, 520 U.S. at 314. Far from being "minimal," plaintiffs' privacy interests in their Internet activities and communications lie at the heart of the Fourth Amendment. A person's Internet activities encompass a vast array of intimate details about that person's private life. *See* Plaintiffs' Motion (ECF No. 261) at 12-14.

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, for example, schoolchildren who voluntarily choose to participate in extracurricular activities, *see Bd. of Educ. of Indep. Sch. Dist. No. 92 of Pottawatomie Cnty. v. Earls*, 536 U.S. 822, 830-32 (2002); *Vernonia Sch. 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; *Nat'l 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*, 532 U.S. at 90-91 (Kennedy, J., concurring).

Here, plaintiffs have an *undiminished* expectation of privacy in the content of their electronic 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 that the government seizes and searches could not be more complete—the government seizes all of plaintiffs' communications flowing through AT&T's Internet backbone connections and searches the entire contents of millions of those communications, every word from top to bottom.

None of the Supreme Court's decisions approving special needs searches involved circumstances remotely similar to those present here. None of those cases involved the suspicionless content-searching of papers or communications. None of those cases involved seizures and searches of the vast scale and magnitude occurring here, extending across the breadth of American society. Testing student athletes or train operators for drug use or checking automobile drivers for sobriety is nothing like searching the contents of the Internet communications of millions of ordinary Americans.

On the other side of the balance, the government asserts that its interest in acquiring foreign intelligence information is of the "highest order." Govt. Opp. (ECF No. 285) at 39. But the government's interest in acquiring foreign intelligence information, weighty as it is, does not give it a blank check to use any and every means of surveillance to pursue that interest with no regard for how deep and widespread the intrusion into the privacy of innocent Americans. *Al Haramain*, 686 F.3d at 993 ("government's interest in preventing terrorism," while "extremely high," "is no excuse for dispensing altogether with domestic persons' constitutional rights"). The balance here weighs in favor of plaintiffs.

The government also has failed to satisfy the primary-purpose test. Strikingly, the government does not contend that the primary purpose of its Internet backbone surveillance is to collect foreign intelligence information. Instead, it goes no further than asserting that foreign

intelligence collection is "a 'significant purpose'" of its Internet backbone surveillance, quoting the language of section 702. Govt. Opp. (ECF No. 285) at 36-37; *see id*. at 37 n.10 (asserting only that "the Section 702 program serves the Government's need to obtain foreign intelligence" while also promoting other interests). This is not surprising; the government has confirmed that it retains not only foreign intelligence information, but also any information that is evidence of a crime or indicates an imminent threat of death or serious bodily harm, all of which are ordinary law enforcement concerns. ECF No. 253-7 at 8-9, 11. Indeed, the FBI routinely searches communications collected by the NSA's Internet backbone surveillance when investigating ordinary crimes. ECF No. 262, Ex. A at 137 (7/25/14 Wiebe Decl.).

The government's invocation of the special needs exception additionally fails because it has made no attempt to show that it lacks other practicable alternatives to the mass suspicionless seizures and searches occurring here. The government may believe that mass surveillance is a more convenient method of detecting wrongdoing or ferreting out information (a question certainly open to dispute), but if the Fourth Amendment could be overcome by a showing of mere convenience alone, privacy would cease to exist. Alternatives do exist, and the government is using them. For example, similar to a traditional wiretap, the government has methods by which it can and does collect only the communications actually transmitted to and from phone numbers, email accounts, and websites belonging to individuals and organizations it has targeted for foreign intelligence surveillance. The government's PRISM surveillance, in which by the government's description it obtains communications to and from, for example, specific Yahoo! email accounts or specific Facebook accounts, appears to be an example of this. ECF No. 262, Ex. A at 7, Ex. B (7/25/14 Wiebe Decl.); 10/24/14 Wiebe Decl., Ex. A at 33-34. So, too, is the government's surveillance under traditional FISA surveillance orders issued under 50 U.S.C. §§ 1804-1805 or under its emergency surveillance powers under 50 U.S.C. §§ 1802 and 1805(e). The government's interception of telephone calls to and from phone numbers of foreign powers and agents of foreign powers under a traditional FISA order avoids suspicionless searches and seizures of calls to the phone numbers of innocent Americans. While some of these forms of surveillance may raise their own concerns, there is no doubt that what the government does here is far broader, no different than

listening to every telephone call in the country to see if anyone happens to mention a telephone number associated with a surveillance target. Thus, it is not impracticable to use methods other than mass Internet backbone surveillance to intercept communications that are actually to or from targeted persons.

To the extent the government contends it is impracticable to use a warrant to conduct mass suspicionless surveillance of the communications of millions of innocent Americans, that is not because a necessity for speed or some other exigency stands as an impediment to obtaining a warrant or court order in a timely fashion. It is because the government's goal of seizing and searching through the communications of millions of innocent Americans without suspicion is an illegitimate goal that flies in the face of the Fourth Amendment itself—which, at its "very heart" "forbids searching a person for evidence of a crime when there is no basis for believing the person is guilty of the crime or is in possession of incriminating evidence." *Maryland v. King*, __ U.S. __, 133 S. Ct. 1958, 1980 (2013) (Scalia, J., dissenting).

The government attempts to carry its burden of showing impracticability by relying solely on statements in legislative reports and hearings, but those statements are inadmissible hearsay. Fed. R. Evid. 801(c), 802. Moreover, those statements are insufficiently specific, since they speak only generally about surveillance pursuant to the FISA Amendments Act (which added section 702 to FISA), and do not discuss specifically the Internet backbone surveillance that plaintiffs challenge. The government has admitted conducting two different types of surveillance under section 702: PRISM and Internet backbone surveillance (which it also calls "Upstream"). ECF No. 262, Ex. A at 7 (7/25/14 Wiebe Decl.). PRISM interceptions are limited to specific communications accounts (e.g., email accounts, Facebook accounts, or websites) used by non-U.S. persons to communicate foreign intelligence information. ECF No. 262, Ex. A at 7 (7/25/14 Wiebe Decl.); 10/24/14 Wiebe Decl., Ex. A at 33-34. Internet backbone surveillance indiscriminately intercepts all the communications and Internet traffic flowing through key junctions on the Internet backbone, and is not limited to communications by non-U.S. persons or foreign intelligence information. ECF No. 262, Ex. A at 7, 35-37 (7/25/14 Wiebe Decl.). So a statement on the importance of surveillance

under the FISA Amendments Act or section 702 says nothing about the specific significance of the Internet backbone seizures and content searching that plaintiffs challenge.

B. The Decisions On Which The Government Relies Do Not Support A "Special Needs" Exception For Mass Suspicionless Internet Surveillance

The foreign-intelligence special needs decisions on which the government relies do not support the conclusion that its Internet backbone surveillance satisfies the special needs exception. Because the special needs analysis is a context-specific inquiry, the conclusion that *one* form of foreign intelligence gathering might, on its particular facts, be exempt from the warrant requirement does not suggest that *all* forms of foreign intelligence gathering are exempt from the warrant requirement. *See Chandler*, 520 U.S. at 313-14; *compare Michigan Dept. of State Police v. Sitz*, 496 U.S. 444, 455 (1990) (warrantless roadblock was permissible under Fourth Amendment) *with Edmond*, 531 U.S. at 41-42 (warrantless roadblock violated Fourth Amendment).

The decisions on which the government relies do not address its mass suspicionless Internet backbone surveillance but involve interception only of designated telephone numbers, email accounts, or other specified communications accounts used by a foreign power or an agent of a foreign power. *See U.S. v. Duka*, 671 F.3d 329, 338 (3d Cir. 2011) (electronic surveillance of several defendants pursuant to a traditional FISA order under 50 U.S.C. § 1805); *In re Sealed Case*, 310 F.3d 717, 720 (Foreign Int. Surv. Ct. Rev. 2002) (review of traditional FISA order under 50 U.S.C. § 1805); *U.S. v. Truong Dinh Hung*, 629 F.2d 908, 911-12 (4th Cir. 1980) (pre-FISA wiretapping and bugging of the telephone and apartment of an agent of a foreign power); *U.S. v. Buck*, 548 F.2d 871, 875 (9th Cir. 1977) (pre-FISA wiretap of a single phone line); *U.S. v. Bin Laden*, 126 F. Supp. 2d 264, 269 (S.D.N.Y. 2000) (telephone wiretap and search of home of American citizen living in Kenya based on individualized suspicion linking him to al Qaeda), *aff'd sub nom. In re Terrorist Bombings of U.S. Embassies in E. Africa*, 552 F.3d 157 (2d Cir. 2008). Moreover, *In re Sealed Case* has no precedential value because, like a magistrate judge's decision granting a search warrant, it is not the product of an Article III adversary proceeding.

Equally irrelevant are decisions relating to surveillance conducted under the government's PRISM program, which by the government's description is limited to specific communications

accounts. For example, *In re Directives to Yahoo! Inc.*, FISC-R No. 08-01 (Foreign Int. Surv. Ct. Rev., Aug. 22, 2008),[11] addresses only PRISM surveillance of specific Yahoo! communications accounts, not the mass suspicionless Internet backbone surveillance. *See In re Directives to Yahoo! Inc*, FISC-R No. 08-01, Yahoo! Inc.'s Opening Brief at 54-55 (5/29/08) (describing surveillance of specific Yahoo! accounts); *In re Directives to Yahoo! Inc*, FISC No. 105B(G) 07-01,Yahoo! Inc.'s Compliance Report at 2 (5/14/2008) (discussing Yahoo! "user accounts" the government designate for surveillance);[12] *accord [Redacted Caption]*, 2011 WL 10945618 at *27 n.67 (FISC, Oct. 3, 2011) ("The dispute in *In re Directives* involved the acquisition by NSA of discrete to/from communications from an Internet Service Provider, not NSA's upstream collection"). Yahoo! is a participant in PRISM surveillance but does not operate Internet backbone facilities. *See* ECF No. 262, Ex. B (7/25/14 Wiebe Decl.).

U.S. v. Mohamud, 2014 WL 2866749 (D. Or. June 24, 2014), also provides no support for the government here. *Mohamud* rejected an as-applied challenge to section 702 by a defendant convicted of terrorism charges. It did not purport to analyze the constitutionality of the government's intentional—and suspicionless—Internet backbone surveillance of the communications of innocent Americans. *Mohamud* did not address the constitutionality of either the initial suspicionless mass interceptions or the content searching that plaintiffs challenge here. It is not even clear that the *Mohamud* court knew whether or not the section 702 surveillance at issue occurred under PRISM or was Internet backbone surveillance, or knew whether the defendant was a target of the surveillance or not, for the court denied the defendant any discovery relating to the surveillance. Even on the question it did decide, *Mohamud's* analysis is inconsistent with *Riley v. California*, decided by the Supreme Court the day after *Mohamud*. 573 U.S. __, 134 S. Ct. 2473 (2014). *Mohamud's* fundamental rationale is that the government's targeting and minimization procedures are an adequate substitute for a warrant. That conclusion is in irreconcilable conflict

[11] The government cites to the superseded 2008 redacted version of the opinion (551 F.3d 1004), but a more complete version was released in September 2014 and is available at http://www.dni.gov/files/documents/0909/FISC Merits Opinion 20080822.pdf.

[12] Available at http://www.dni.gov/files/documents/0909/Yahoo Compliance Report 20080514.pdf.

with the Supreme Court's admonition that "government agency protocols" are no substitute for a warrant. *Riley*, 134 S. Ct. at 2491.

The government's final remaining authority, *[Redacted Caption]* (cited in plaintiffs' opening brief as "[Name and docket no. redacted]" and "10/3/11 FISC Opinion," *see* Plaintiffs' Motion (ECF No. 261) at 4 n.3), is equally unpersuasive. Like *In re Sealed Case*, it lacks precedential value because it was not the product of an Article III adversary proceeding but of a one-sided ex parte process; it is not even an advisory opinion. Its conclusion is that Internet backbone surveillance as it operated in 2011 *violated* the Fourth Amendment in certain respects. 2011 WL 10945618 at *28-*30. It made no independent analysis of whether that seizure and searching of the communications of innocent Americans violated the Fourth Amendment, deferring instead to an earlier FISC opinion that has never been released. *Id*. at *24 ("The Court has previously concluded that the acquisition of foreign intelligence information pursuant to Section 702 falls within the 'foreign intelligence exception' to the warrant requirement of the Fourth Amendment. *See* Docket No. [redacted]."). Because *[Redacted Caption]* does not explain the reasoning of that earlier secret opinion, it adds no weight to the government's arguments.

IV. Even If The Warrant Requirement Did Not Apply Here, The Mass Seizures And Searches The Government Conducts Here Are Unreasonable

As the plaintiffs' motion explains, warrantless searches and seizures are presumptively unreasonable. Even where an exception to the warrant requirement exists, a search or seizure must still meet the Fourth Amendment's test of reasonableness. The test of reasonableness, like the special needs analysis, balances the intrusion on plaintiffs' interests against the strength of the government's interest, while also looking at the effectiveness of the intrusion at advancing the government's interest.

"Whether a search is reasonable 'is determined by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.'" *Samson v. California*, 547 U.S. 843, 848 (2006); *accord Al Haramain*, 686 F.3d at 994. The government agrees it must meet this standard in addition to meeting the special needs exception. Govt. Opp. (ECF No. 285) at 38.

Here, the government's argument fails at the outset because plaintiffs have an undiminished expectation of privacy and because their privacy is invaded by the government's seizure and top-to-bottom searching of their communications. The Ninth Circuit's analysis in *Al Haramain* is equally applicable here: "The cases in which the [Supreme] Court has found warrantless searches to be reasonable all involve very special circumstances and greatly diminished privacy interests—a point repeatedly emphasized by the Court. . . . Here, however, as we have explained, the reach of [the government's seizure] authority extends to *all persons and entities,* without limitation. Nothing diminishes the privacy expectation of persons and entities potentially subject to seizure by [the government] because that class includes everyone." *Al Haramain*, 686 F.3d at 994 (italics original). So too here, the government's seizures and searches are not limited to persons with diminished privacy interests but extend to everyone.[13]

The government attempts to denigrate plaintiffs' privacy interests by arguing that its search is only a "fleeting electronic scanning" that is only "a minimal intrusion, if any, on Plaintiffs' possessory and privacy interests." Govt. Opp. (ECF No. 285) at 39. But the duration of these searches says nothing about their intrusiveness, unlike some of the contraband searches. The government's rhetoric cannot paper over the fact that its searches, no matter how swiftly completed, examine the complete contents of a communication from top to bottom.

The government also contends that section 702's significant-foreign-intelligence-purpose requirement and its targeting procedures diminish the intrusion upon plaintiffs' interests. Govt. Opp. (ECF No. 285) at 39-40. This is a non sequitur; the objective intrusiveness of a search is not diminished by the subjective purposes or intentions of the searcher. And, in any event, the government's claim that its "targeting" is limited to non-U.S. persons located overseas is meaningless in light of the fact that it intentionally searches the contents of every American's international communications. Equally off base is the government's contention that reports by the

[13] In *Maryland v. King*, the Supreme Court expressly conditioned its finding that Maryland's DNA testing of arrestees was reasonable on the fact that it applied only to individuals who had a diminished expectation of privacy because they had been lawfully arrested for a serious offense supported by probable cause. 133 S. Ct. at 1978-79.

Executive to Congress and the FISC on its compliance with its targeting procedures diminish the intrusion on plaintiffs' privacy. *Id*. at 40. A report to Congress or a court cannot diminish the objective intrusiveness of a search.[14]

Finally, the government seeks to show that Internet backbone surveillance is a "reasonably effective means" for advancing its national security interests by again citing inadmissible hearsay in legislative reports. Govt. Opp. (ECF No. 285) at 40-41. These hearsay reports, like others the government cites, address only section 702 generally, and not Internet backbone surveillance. They certainly do nothing to show that searching the communications of innocent Americans that are not sent to or received from a surveillance target is a "reasonably effective means" of advancing the government's national security interests. The government then asserts that "[t]he Executive Branch's assessment of the value and importance of intelligence-gathering activities under the FAA [FISA Amendment Acts] is 'entitled to deference'" (*id*. at 41), but it cites no such Executive assessments, much less submits them in an admissible form. And the mere fact that Congress has enacted and reenacted section 702 is no substitute for "empirical evidence" of the effectiveness, not of section 702 in general, but of the specific Internet backbone surveillance practices that plaintiffs are challenging. *Sitz*, 496 U.S. at 454; *U.S. v. Scott*, 450 F.3d 863, 870 (9th Cir. 2005) (effectiveness requires an "empirical demonstration"). Moreover, section 702, for its part, far from endorsing mass suspicionless searches of the sort occurring here, says nothing at all about them.

Mass suspicionless searches and seizures are the "immediate evils" the Fourth Amendment was designed to protect against. *Payton v. New York*, 445 U.S. 573, 583 (1980). For all the reasons stated above and in plaintiffs' motion, the Fourth Amendment leaves no room for mass suspicionless seizures and searches of the contents of communications of millions of innocent Americans.

[14] Also meritless is the government's contention that its mass suspicionless Internet backbone surveillance of the communications of innocent Americans like plaintiffs is less of a Fourth Amendment intrusion than the much narrower PRISM seizures at issue in *In re Directives*, which are limited to specific communications accounts used by non-U.S. persons to communicate foreign intelligence information, and the unknown seizures in *Mohamud*. Govt. Opp. (ECF No. 285) at 39.

V. The Government's Evidentiary Challenges To The Klein And Marcus Declarations Lack Merit, And Plaintiffs' Evidence Supports Summary Judgment

The government's evidentiary challenges miss their mark. Along with a wide array of other evidence including the government's and AT&T's own admissions, plaintiffs rely on declarations by former AT&T employee Mark Klein, expert Scott Marcus, and AT&T Managing Director James Russell, together with the AT&T documents that are exhibits to Klein's declaration (the "AT&T documents"), to demonstrate the mass surveillance at issue here and AT&T's participation in it. But given the narrow scope of plaintiffs' motion and the government's and AT&T's admissions, plaintiffs' motion cites and relies on only limited portions of the Klein and Marcus declarations. All of those portions are admissible.

The government does not even attempt to contest most of the essential facts here. The government admits that: "NSA collects telephone and electronic communications as they transit the Internet 'backbone' within the United States."[15] Other undisputed evidence also confirms this fact.[16] It is also beyond dispute that AT&T conducts surveillance for the NSA under the Foreign Intelligence Surveillance Act, as AT&T itself admits. 10/24/14 Wiebe Decl., Ex. B. Other evidence also confirms AT&T's participation. *See* Plaintiffs' Motion (ECF No. 261) at 10-11 and evidence cited therein.

It is also undisputed that the communications copied in bulk from the Internet backbone are filtered and the remaining communications are then searched from top to bottom (stages two and three). *See* Plaintiffs' Motion (ECF No. 261) at 6-9 and evidence cited therein.

The government also does not dispute Klein's testimony regarding the splitters installed at AT&T's San Francisco and use of the splitters to copy AT&T's Internet backbone traffic and divert

[15] ECF No. 227 at ¶ 38, 25:14-16 (12/20/13 NSA Deputy Dir. Fleisch Classified Decl.)

[16] ECF No. 169 at 17 (12/20/13 NSA Deputy Dir. Fleisch Unclassified Decl.); ECF No. 253-3 at 3 (6/27/14 Gilligan Decl., Ex. B); ECF No. 262, Ex. A at 7, 35-37, Ex. B at 3-4 (7/25/14 Wiebe Decl.); ECF No. 174-1 at 26 (1/10/14 Rumold Decl., Ex. 1); Memorandum Opinion ("10/3/11 FISC Opinion"), [Name and docket no. redacted], 2011 WL 10945618, at *2 n.3 (FISC Oct. 3, 2011).

the copies into the secret SG3 Secure Room (stage one).[17] It hardly could contest this testimony, for Klein was personally in charge of the operation and maintenance of the splitters and the fiber-optic cables between the splitters and the SG3 Secure Room.

The government nonetheless contends that plaintiffs' evidence showing the government's involvement in the copying and diversion of the communications transiting AT&T's Internet backbone network, the existence of splitters on AT&T's backbone network in other cities, and the electronic devices that are within the SG3 Secure Room is not admissible. Govt. Opp. (ECF No. 285) at 14-16. Significantly, the government does not submit any evidence to the contrary that would create a genuine factual dispute; it contends only that plaintiffs' evidence on these points either lacks foundation or is hearsay and therefore is inadmissible.

The government's contentions lack merit, for plaintiffs' evidence meets the evidentiary standard for summary judgment: At this stage, the question is whether plaintiffs' evidence could be presented in an admissible form at trial, not whether it is currently in an admissible form. Fed. R. Civ. P. 56(c)(2); *Fonseca v. Sysco Food Servs. Of Ariz., Inc.*, 374 F.3d 840, 846 (9th Cir. 2004); *Fraser v. Goodale*, 342 F.3d 1032, 1036-37 (9th Cir. 2003). The portions of the Klein and Marcus declarations that plaintiffs rely upon for this motion are grounded in Klein's own observations and activities in the course of his job duties at AT&T over many years and Marcus's unchallenged expertise in the telecommunications field, and the information in the AT&T documents is independently attested to not just by Klein but by Russell. Moreover, the statements of AT&T employees regarding the NSA's control and direction of the Internet backbone interceptions are admissible nonhearsay.

A. Mark Klein's Declaration Is Based On His Personal Knowledge And Experience At AT&T

Federal Rule of Evidence 602 requires that testimony be based on personal knowledge, but "the threshold of Rule 602 is low." *U.S. v. Hickey*, 917 F.2d 901, 904 (6th Cir. 1990). Personal

[17] ECF No. 84-2 at ¶¶ 21-34 (Klein Decl.); ECF Nos. 84-3, 84-4, 84-5, 84-6 (Klein Decl., Exs. A, B, C); ECF No. 89 at ¶¶ 56-58, 62, 70-73, 77, 109 (Marcus Decl.); ECF No. 84-1 at ¶¶ 6, 10-12, 15, 19-23 (Russell Decl.).

knowledge need not be expressly stated but can be inferred from the declaration itself. *Barthelemy v. Air Lines Pilots Ass'n*, 897 F.2d 999, 1018 (9th Cir. 1990). In particular, in the case of testimony by employees about their company's business operations, "personal knowledge and competence to testify are reasonably inferred from their positions and the nature of their participation in the matters to which they swore." *Id*. Moreover, "[p]ersonal knowledge can include 'inferences and opinions, so long as they are grounded in personal observation and experience.'" *U.S. 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); *accord U.S. v. Famania-Roche*, 537 F.3d 71, 76 (1st Cir. 2008) (low-level drug dealer could testify to activities and drug sales by other drug dealers in narcotics organization she was part of); *DIRECTV, Inc. v. Budden*, 420 F.3d 521, 529 (5th Cir. 2005) (employee could testify about facts concerning another company he learned through a law enforcement investigation); *U.S. v. Doe*, 960 F.2d 221, 223 (1st Cir. 1992) (gun shop owner could testify that pistol was manufactured in Brazil without stating the basis for his inference); *Great Am. Assur. Co. v. Liberty Surplus Ins. Corp.*, 669 F. Supp. 2d 1084, 1089 (N.D. Cal. 2009) (employee can testify to company policies based on her "experience and perceptions" on the job); *Sjoblom v. Charter Commc'ns, 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); *U.S. 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). *See also* Fed. R. Evid. 701 (lay opinion).

Klein's declaration is solidly grounded in his own personal knowledge, based on his decades of experience with AT&T's business practices and operations and his observations and activities in the course of his employment. Klein's job at AT&T's Folsom Street facility included "oversee[ing] the WorldNet Internet room" (ECF No. 84-2 at ¶ 15 (Klein Decl.)), and he attests that Internet backbone communications data under his oversight was copied and sent over fiber-optic cables into

the SG3 Secure Room. *Id*. at ¶¶ 27, 34. Indeed, Klein *himself* was responsible for connecting Internet backbone circuits to the splitter cabinet, as directed by the AT&T documents that he relied on to do his job. *Id*. at ¶¶ 36, 25, 26 & Exs. A-C. Klein also gives detailed descriptions of Internet backbone circuits he knew to be copied and diverted into the SG3 Secure Room and the types of data carried on those circuits. *Id*. at ¶¶ 19, 22, 28-34. All of this information is squarely within his personal knowledge and experience and is admissible evidence that satisfies Rule 602. *See Barthelemy*, 897 F.2d at 1018. [redacted]

B. The Evidence That The Splitter Is Part Of The Government's Internet Backbone Surveillance Is Admissible

Klein's testimony of the NSA's involvement at the Folsom Street Facility where he worked is admissible on numerous grounds.

First, Klein's testimony is based on his observations and experiences on the job, and is no different in substance than the testimony of an employee regarding his observations of his company's interactions with a particular customer or another company. The Court has no doubt many times admitted testimony of this sort, for it is a staple of commercial litigation.

For example, Klein, who otherwise had keys and free access to all parts of AT&T's Folsom Street Facility, was excluded from only the SG3 Secure Room because AT&T's policy was to restrict access to the room to only persons cleared by the NSA, even in emergencies. ECF No. 84-2 at ¶¶ 17, 18 (Klein Decl.). This testimony is based on Klein's personal knowledge, observations, and experiences of AT&T's business operations and its policies and practices, and his observations of its employees. *See Neal*, 36 F.3d at 1206; *Great Am. Assur. Co.*, 669 F. Supp. 2d at 1089; *Sjoblom*, 571 F. Supp. 2d at 968-69. So, too, is Klein's testimony of visiting the SG3 Secure Room while it was under construction (where he saw AT&T employee "FSS #2," who had met with an NSA agent, installing equipment) and of again visiting the room after it was in operation. ECF No. 84-2 at ¶¶ 10, 12, 14, 17 (Klein Decl.).

Second, 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,[18] 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. U.S.*, __ F. Supp. 3d __, 2014 WL 4928959, at *4 n.3 (E.D. Ky. Sept. 30, 2014); *Quintero v. U.S.*, 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 Commc'ns Integrated Sys. v. U.S.*, 91 Fed. Cl. 347, 359 (Fed. Cl. 2010); *Globe Sav. Bank, F.S.B. v. U.S.*, 61 Fed. Cl. 91, 93-95 (Fed. Cl. 2004). Because the statements were made at a time when AT&T and the government were violating not only the Fourth Amendment but also FISA, the statements are also admissible as statements by a coconspirator. Fed. R. Evid. 801(d)(2)(E).

In addition to being admissible under Rules 801(d)(2)(D) and (d)(2)(E), 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, that the purpose of the first meeting was that "the NSA agent was to interview FSS #2 for a special job" and that the purpose of the second meeting was to discuss "FSS #3's suitability to perform the special job that FSS #2 had been doing," that AT&T's management's plan and intent was to cooperate with the NSA, and that AT&T thereafter did cooperate with the NSA. Fed. R. Evid. 803(3) (statements reflecting plan or intent are admissible); *U.S. 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"). And Klein's statements that "The NSA agent came and met with FSS #2" and "The NSA agent did come and speak to FSS #1" are personal observations. ECF No. 84-2 at ¶¶ 10, 16 (Klein Decl.).

C. The Evidence That Similar Splitters Exist At Other Locations Is Admissible

The evidence that similar splitters exist at other locations on the AT&T backbone network is admissible. The statement of an AT&T employee that splitters exist in other cities, including Seattle, San Jose, Los Angeles, and San Diego (ECF No. 84-2 at ¶ 36 (Klein Decl.)), is admissible

[18] *See* 10/24/14 Wiebe Decl., Ex. B.

nonhearsay by an agent. Fed. R. Evid. 801(d)(2)(D). One of the AT&T documents also demonstrates that there are four different styles of splitter cabinets used by AT&T, and thus at least four different locations where AT&T's backbone network is being intercepted. ECF No. 84-2 at Ex. A (Klein Decl.); ECF No. 89 at ¶¶ 113-118 (Marcus Decl.). The document also discloses that there is a splitter located in Atlanta. ECF No. 84-2 at Ex. A at A-17 (Klein Decl.). The AT&T documents are admissible as AT&T business records, as both Klein and Russell make clear, and as statements by AT&T as the government's agent. Fed. R. Evid. 801(d)(2)(D), 803(6); *see* ECF No. 84-2 at ¶¶ 25-26, 28 (Klein Decl.); ECF No. 84-1 at ¶¶ 5-6, 20-22 (Russell Decl.).

D. The Evidence Of The Electronic Devices In the SG3 Secure Room Is Admissible

For purposes of this motion only, plaintiffs accept the government's representation that after it copies communications from the Internet backbone it filters them and then searches them at stages two and three. *See* Plaintiffs' Motion (ECF No. 261) at 5-9 and evidence cited therein. Whether that filtering and searching occurs in the SG3 Secure Room or elsewhere, and what electronic devices are used to perform the filtering and searching, are irrelevant to plaintiffs' Fourth Amendment claim. Nonetheless, even though it is not essential to their motion, the evidence plaintiffs present regarding the electronic devices in the SG3 Secure Room is admissible.

Klein's testimony regarding the electronic devices in the SG3 Secure Room that were attached to the other end of the fiber-optic cables he was responsible for maintaining is based on the AT&T documents he relied on to do his job, which are themselves admissible business records and admissions. ECF No. 84-2 at ¶¶ 28, 35 & Ex. C (Klein Decl.). [redacted]

E. The Marcus Declaration Is Admissible Expert Testimony

Marcus's expert declaration is based on evidence within the Klein declaration and the AT&T documents, as well as the other evidence Marcus cites and Marcus's own extensive personal experience with and specialized knowledge of the telecommunications networking field and related business practices and economics—all of which he sets forth in his declaration.

The government challenges Marcus's expert testimony because he lacks "personal knowledge" and relies on Klein's testimony. Govt. Opp. (ECF No. 285) at 17. But Marcus, like any expert, is not limited to his personal knowledge and can rely on the testimony and evidence of others, including hearsay and other forms of evidence that would themselves be inadmissible. Fed. R. Evid. 703. And the government does not challenge Marcus's qualifications to assess the operation and implications of the splitter cabinet and related equipment. In any event, all of the Klein evidence that Marcus relies upon is competent for the reasons explained above. Moreover, Marcus does not rely on statements made by others that Klein reports, including statements regarding the NSA.

The government also challenges Marcus's qualifications to support his opinion that the government (not AT&T) funded the SG3 Secure Room, claiming that Marcus did not "consider himself an economist" and "has had no economics or corporate finance training." Govt. Opp. (ECF No. 285) at 18. But plaintiffs' motion does not depend on who paid for the secret room. And Marcus has more than adequate qualifications to render this opinion.

Marcus first concluded that AT&T had no technical or business reason for installing the splitter and sending complete copies of communications transiting its Internet backbone to the SG3 Secure Room. ECF No. 89 at ¶¶ 41-49, 128-139 (Marcus Decl.). The government does not challenge this conclusion, and it is well within Marcus's expertise. Marcus then examined AT&T's declining revenues and profits and other evidence of AT&T's weak financial condition at the time the SG3 Secure Room was installed–facts that the government does not attempt to rebut or contest. *Id*. at ¶¶ 140-147. He concluded that given the lack of a business or technical purpose for the SG3 Secure Room, it was unlikely that AT&T would have funded its installation it at a time when AT&T was financially weak. *Id*. This common-sense conclusion is also within Marcus's expertise in the field of economic and business aspects of telecommunications networks—a field in which Marcus

has decades of relevant experience, including authoring multiple papers involving economic issues in this field and serving as the Senior Advisor for Internet Technology at the Federal Communications Commission, AT&T's chief regulator. *Id*. at ¶¶ 7, 13-18 (network design and capacity planning experience, including economic analysis), ¶¶ 24, 27, 29 (experience and economic knowledge related to telecommunications and experience authoring economic papers).

At bottom, the government's objections to Marcus's testimony go its weight, not its admissibility. But the ordinary method for challenging the weight of an expert's testimony is to submit contrary expert testimony, which the government does not do. In any event, what matters is not who paid for the room but that the installations and operations that Klein describes and Marcus opines about are entirely consistent with the government's recently disclosed descriptions of its surveillance operations, were conducted in secrecy that had no part in AT&T's normal business practices, and trace the specific connection between telecommunications services that plaintiffs use and the physical mechanism that initiates the government's surveillance process.

F. Plaintiff's Evidence Is Not Inadmissible As "Stale"

Finally, the government's contention that Klein or Marcus's evidence is inadmissible because it is somehow "stale" has no basis in fact or law. First, the government admits that its interception, filtering, and searching of communications from the Internet backbone is active and ongoing. *See* Plaintiffs' Motion (ECF No. 261) at 6-9 and evidence cited therein. Given that admission, the "staleness" argument fails utterly.

Second, the government cites no authority showing that any such "freshness" rule exists in the context of a civil party's summary judgment motion. Both decisions the government cites address only whether "stale" evidence is sufficient to provide the reasonable suspicion or probable cause necessary to support a search or seizure—an entirely different question from whether evidence is admissible to help establish a relevant fact in a civil case. *Ortega v. O'Connor*, 146 F.3d 1149, 1162 (9th Cir. 1998) (considering whether an uncorroborated allegation of a one-time event 10 years earlier in which plaintiff had acted inappropriately gave defendants reasonable suspicion to search plaintiff's office); *Szajer v. City of Los Angeles*, 632 F.3d 607, 612 (9th Cir. 2011) (considering whether events from five and fifteen years earlier demonstrated probable cause for a warrant). They were rulings about the weight of evidence, not its admissibility. Unrebutted evidence of an ongoing

pattern and practice of unconstitutional conduct like plaintiffs' evidence here is admissible and supports an inference that the conduct is continuing.[19]

VI. The State Secrets Privilege Provides No Defense

The state secrets privilege has no application here for multiple reasons. First, it has no application because plaintiffs' motion is based solely on public evidence. Even where the government successfully asserts the state secrets privilege, the only result is "[t]he privileged information is excluded and the trial goes on without it." *General Dynamics Corp. v. U.S.*, __ U.S. __, 131 S. Ct. 1900, 1906 (2011). "[T]he effect of the government's successful invocation of privilege 'is simply that the evidence is unavailable, as though a witness had died, and the case will proceed accordingly, with no consequences save those resulting from the loss of evidence.'"[20] *Al Haramain Islamic Foundation, Inc. v. Bush*, 507 F.3d 1190, 1204 (9th Cir. 2007); *Kasza v. Browner*, 133 F.3d 1159, 1166 (9th Cir. 1998) ("The plaintiff's case then goes forward based on evidence not covered by the privilege.").

Plaintiffs' evidence is entirely public; it principally consists of public admissions by the government regarding its Internet backbone surveillance and the Klein and Marcus declarations and documents. The government long ago waived any privilege in any of the matters set forth in the Klein and Marcus evidence, including the documents attached to the Klein declaration. *See Hepting*, 439 F. Supp. 2d at 989; 10/24/14 Wiebe Decl., Ex. C (6/23/06 Hearing Tr., *Hepting v. AT&T Corp.*, N.D. Cal. No. 06-cv-0672-VRW, ECF No. 284). "Operational details," such as the identities of the government's surveillance targets, are irrelevant to the merits of plaintiffs' claims, and would not be revealed by a ruling in plaintiffs' favor.

---

[19] The government also argues that media reports are inadmissible, but plaintiffs do not rely on media reports alone for any fact essential to their motion. They are cited only for general background.

[20] The "full and fair adjudication" standard that the government puts forward is not the law. Govt. Opp. (ECF No. 285) at 45. Every evidentiary privilege—indeed, every rule that excludes relevant evidence—potentially makes the resulting adjudication something less than full and fair. Nonetheless, as with other privileges, when the state secrets privilege causes evidence to be excluded, the case proceeds using the remaining public evidence. *General Dynamics*, 131 S. Ct. at 1906.

Second, the Court has already ruled that 50 U.S.C. § 1806(f) displaces the state secrets privilege with respect to plaintiffs' statutory claims, and the government has conceded that "the reasoning by which the Court concluded that section 1806(f) preempts application of the privilege to Plaintiffs' statutory claims would apply equally to Plaintiffs' constitutional claims." 7/23/13 Order (ECF No. 153) at 12-13; ECF No. 167 at 2, 6-7. So the government's attempt to assert the state secrets privilege here is precluded by section 1806(f) and the Court's prior ruling.

Third, the government's attempt to invoke the valid-defense exception under the state secrets privilege fails. The government contends that it would use the secret evidence in the Miriam P. declaration (ECF No. 288) to "raise and support defenses in addition to" the defenses already raised in its opposition. Govt. Opp. (ECF No. 285) at 45. Whatever those hypothetical undisclosed defenses are, the Court's section 1806(f) ruling requires that the government must use section 1806(f)'s procedures if it contends secret evidence would show that the surveillance was lawful. Moreover, even if the state secrets privilege rather than section 1806(f) governed here, the valid-defense exception would not apply because it is limited to government contracting cases. ECF No. 112 at 14-16. Further, even if the state secrets privilege and the valid-defense exception both did apply here, they would require the government to submit evidence proving up a "demonstrably valid," and not just "plausible" or "colorable," defense. *In re Sealed Case*, 494 F.3d 139, 149-51, 153 (D.C. Cir. 2007); *see* ECF No. 112 at 28-29. Plaintiffs submit that the government has not proven up any "demonstrably valid" defense.

The government makes one other stab at invoking the state secrets privilege, arguing that it precludes any adjudication of plaintiffs' standing. Govt. Opp. (ECF No. 285) at 21-23. Part of its argument is just a repetition of its sufficiency-of-the-evidence argument asserting that plaintiffs have not proven that AT&T participates in the government's Internet backbone surveillance. *Id*. at 22. But as plaintiffs' motion explains, the Klein and Marcus evidence, as well as other evidence, establishes AT&T's participation in Internet backbone surveillance. Further evidence that AT&T's participation is not secret are the transparency reports AT&T now issues confirming that its customers' accounts are subject to FISA surveillance. 10/24/14 Wiebe Decl., Ex. B; ECF No. 203 at 5-6 & Ex. A. A ruling based solely on this public evidence discloses no state secrets, especially given the government's privilege waiver and AT&T's own disclosures. And to the extent that the

government wishes to use secret evidence to contest plaintiffs' evidence, it must use section 1806(f)'s procedure. (Because it was not submitted in accordance with section 1806(f), the secret Miriam P. declaration (ECF No. 288), as well as the government's other secret filings, may not be used to decide the merits of plaintiffs' Fourth Amendment claims.) Finally, the government's incomplete quotation from *Clapper v. Amnesty Int'l USA*, __ U.S. __, 133 S. Ct. 1138, 1149 n.4 (2013), omits that the Court's actual concern was limited to disclosure of the identities "on the list of surveillance targets," nothing more. *See* ECF No. 177 at 10-16; ECF No. 203. Granting plaintiffs' motion will disclose nothing about who is a surveillance target.

VII. Plaintiffs' Motion Is Procedurally Proper

Plaintiffs first sought relief from the unlawful surveillance at issue here by filing the related *Hepting* litigation in early 2006. Thereafter, plaintiffs filed this action in 2008. Since this case was filed six years ago, discovery has been completely stayed, even as to nonsecret matters—an unprecedented occurrence in the history of federal civil litigation. It is long past time that this lawsuit moved forward towards a determination on the merits. Plaintiffs' motion advances toward that goal by tendering one issue for decision—their Fourth Amendment claim relating to the government ongoing seizure and searching of communications from the Internet backbone. The public evidence plaintiffs have presented merits a judgment in their favor.

The government seeks to continue avoiding any ruling on the legality of its conduct and argues for further delay and postponement. Its arguments lack merit.

It first argues that any motion should be limited to a determination of plaintiffs' standing. Govt. Opp. (ECF No. 285) at 12. But standing requires a showing that the defendant has caused a legally cognizable harm to the plaintiff—an injury in fact that is legally redressable—and that, and much more, is exactly what plaintiffs' motion demonstrates by proving the government defendants' liability. *See Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560-61 (1992). It would be a senseless and contradictory exercise for the Court to hold that plaintiffs have proven that the government intercepts and searches plaintiffs' communications (thus satisfying the standing components of injury in fact and causation) and that those searches and seizures violate the Fourth Amendment (thus satisfying the standing component of redressability), and yet refuse to use those same findings to hold that the government is liable.

Second, the government argues that plaintiffs' challenge to its Internet backbone surveillance is outside the bounds of the complaint. Govt. Opp. (ECF No. 285) at 12-13. Plaintiffs, however, have always challenged the government's Internet backbone surveillance regardless of the shifting legal theories of Executive or statutory authority the government has asserted in defense of its conduct. *See* ECF No. 233 at 10-14; ECF No. 260 at 2-6. In particular, plaintiffs' Fourth Amendment claim squarely puts in issue the constitutionality of the government's Internet backbone surveillance as it exists today, for its gravamen is that no statute or exercise of Executive authority could constitutionally authorize the surveillance, and thus the government's shifting defenses or a new statute cannot moot this claim.

VIII. The Government's Cross-Motion Should Be Denied

The grounds for the government's cross-motion for summary judgment are the same as for its opposition and lack merit for all of the reasons stated above.

Additionally, however, even if the Court were to deny plaintiffs' motion, that would still not entitle the government to judgment as a defendant, and the government errs in contending otherwise. Govt. Opp. (ECF No. 285) at 13, 20, 21. Plaintiffs' motion is one for partial summary judgment, and it advances just a portion of one of the numerous claims alleged in the complaint. Plaintiffs' motion is based only on the public evidence about the government's Internet backbone surveillance that is currently available. Plaintiffs believe that that evidence is sufficient to establish the specific Fourth Amendment violations raised in their motion. (Contrary to the government's suggestion, plaintiffs do not waive any claims for other Fourth Amendment violations or concede that the government has fully disclosed all of its conduct.) But if the Court disagrees, plaintiffs remain entitled to continue pursuing their Fourth Amendment claims, as well as their other claims, by conducting discovery. The government relies on *Celotex Corp. v. Catrett*, 477 U.S. 317, 322 (1986), but it omits from the sentence it partially quotes the Supreme Court's admonition that a defendant is entitled to summary judgment only "after adequate time for discovery." The Court has thus far denied plaintiffs any discovery whatsoever, and cannot grant summary judgment for the government defendants. *See* Fed. R. Civ. Pro. 56(d); ECF No. 30; ECF No. 114.

CONCLUSION

Plaintiffs' motion for partial summary judgment should be granted and defendants' motion for partial summary judgment should be denied.

Dated: October 24, 2014

Respectfully submitted,

/s/ *Richard R. Wiebe*
RICHARD R. WIEBE
LAW OFFICE OF RICHARD R. WIEBE

CINDY COHN
LEE TIEN
KURT OPSAHL
JAMES S. TYRE
MARK RUMOLD
ANDREW CROCKER
DAVID GREENE
ELECTRONIC FRONTIER FOUNDATION

THOMAS E. MOORE III
ROYSE LAW FIRM

RACHAEL E. MENY
BENJAMIN W. BERKOWITZ
MICHAEL S. KWUN
AUDREY WALTON-HADLOCK
JUSTINA K. SESSIONS
PHILIP J. TASSIN
KEKER & VAN NEST LLP

ARAM ANTARAMIAN
LAW OFFICE OF ARAM ANTARAMIAN

Counsel for Plaintiffs