JOYCE R. BRANDA
Acting Assistant Attorney General

JOSEPH H. HUNT
Director, Federal Programs Branch

ANTHONY J. COPPOLINO
Deputy Branch Director

JAMES J. GILLIGAN
Special Litigation Counsel

MARCIA BERMAN
Senior Trial Counsel

RODNEY PATTON
Trial Attorney

JULIA BERMAN
Trial Attorney

U.S. Department of Justice, Civil Division
20 Massachusetts Avenue, NW, Rm. 6102
Washington, D.C. 20001
Phone: (202) 514-3358; Fax: (202) 616-8470
Email: james.gilligan@usdoj.gov

Attorneys for the Government Defendants

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

OAKLAND DIVISION

CAROLYN JEWEL, *et al.*, Plaintiffs, v. NATIONAL SECURITY AGENCY, *et. al.*, Defendants.	Case No. 4:08-cv-4373-JSW **GOVERNMENT DEFENDANTS' REPLY IN SUPPORT OF THEIR CROSS-MOTION FOR PARTIAL SUMMARY JUDGMENT ON PLAINTIFFS' FOURTH AMENDMENT CLAIM** Date: December 19, 2014 Time: 9:00 a.m. Courtroom 5, Second Floor Hon. Jeffrey S. White

TABLE OF CONTENTS

PAGE

TABLE OF AUTHORITIES

CASES **PAGE(S)**

STATUTES

FEDERAL RULE OF EVIDENCE

LEGISLATIVE MATERIAL

MISCELLANEOUS

INTRODUCTION

Plaintiffs' effort to invalidate NSA[1] "Upstream" acquisition of online communications containing targeted selectors, based on an alleged violation of their Fourth Amendment rights, fails in every way. They adduce no competent evidence of Upstream's operation to support either their standing, or the merits of their claim. Their allegations, even if taken as true, do not establish that alleged Stage 1 copying of online communications, and electronic Stage 3 scanning, result in a seizure and search of the only communications that Plaintiffs put at issue: those that are not retained by the Government, but which, having been found *not* to contain targeted selectors, are instead destroyed within milliseconds of their creation. Even if Plaintiffs had alleged and proven a technical seizure or search under the Fourth Amendment, the minimal intrusion on Fourth Amendment interests caused by the electronic duplication, scanning, and almost immediate destruction of communications that are never seen by Government officials would still be vastly outweighed by Upstream's critical contributions to national security. And although the Government is entitled to judgment for all these reasons based on the public record, in the alternative judgment should be entered for the Government because privileged national security information, subject to the DNI's assertion of the state secrets privilege, is required for a full and fair adjudication of the case, but cannot be disclosed without risking exceptionally grave damage to national security. *See generally* Gov't Mem. Plaintiffs' attempts to sustain their Fourth Amendment claim in the face of these conclusions, *see* Pls.' Opp., meet with no success.

ARGUMENT

I. PLAINTIFFS HAVE ADDUCED NO COMPETENT EVIDENCE TO SUPPORT THEIR STANDING OR THE MERITS OF THEIR CLAIM.

The issue here is whether the Government is "violating the Fourth Amendment by … *ongoing* seizures and searches of *plaintiffs'* Internet communications." Pls.' Mot. at 1 (emphasis added). Thus, while Plaintiffs emphasize that "[t]he [G]overnment admits …'NSA collects telephone and electronic communications as they transit the Internet "backbone" within the

[1] Terminology used but not otherwise defined herein shall have the same meaning as in the Gov't Defs.' Opp. to Pls.' Mot. for Partial Summ. Judg. & Cross-Mot. for Partial Summ. Judg. on Pls.' Fourth Am. Claim (ECF No. 286-6) ("Gov't Mem."). Pls.' Combined Reply in Support of Their Mot. for Partial Summ. Judg. & Opp. to the Gov't Defs.' Cross-Mot. for Partial Summ. Judg. (*see* ECF No. 294) is cited herein as "Pls.' Opp."

United States,'" Pls.' Opp. at 24, 31, the NSA's activities, *in general*, are immaterial to the showing Plaintiffs must make. Rather, Plaintiffs must present admissible evidence that (1) their communications are seized, (2) as part of NSA Upstream collection, (3) on an ongoing basis.

Plaintiffs attempt to meet this burden by arguing that their telecommunications provider, AT&T, "allows the government to seize the entire communications stream of its customers" at Stage 1 of the collection process. Pls.' Mot. at 10; *see* Pls.' Opp. at 3. But this claim depends wholly on the description of the SG3 Secure Room in the Klein and Marcus declarations. *See id.* at 3 n.1; Pls.' Mot. at 6 nn. 5–8. To support Plaintiffs' claim, then, those declarations must, at a minimum, present admissible evidence establishing: (1) that the equipment in the SG3 Secure Room was used for the surveillance activity that Plaintiffs allege; (2) that the NSA received data processed by the equipment in that room; and (3) that the activity Plaintiffs allege took place in 2003 and 2004 remains ongoing. As explained below and in the Government's cross-motion, *see* Gov't Mem. at 14–20, the declarations contain no such evidence.

A. Plaintiffs Have Not Presented Competent Evidence of the Equipment Actually Installed in the SG3 Secure Room or Its Purposes.

Plaintiffs proffer no admissible evidence regarding the equipment allegedly installed in the SG3 Secure Room or the purposes for which it was used. Although Plaintiffs contend that "it is not essential to their motion," Pls.' Opp. at 29, the contents and purpose of the SG3 Secure Room are central to their claim; without such evidence, Plaintiffs' allegations amount to AT&T splitting signals from one room to another at Folsom Street for some unknown purpose.

Plaintiffs cite to paragraphs 24–34 of the Klein Declaration, as well as Exhibits A, B, and C thereto, as the basis for the argument that the equipment allegedly located in the SG3 Secure Room serves the function that they claim. Pls.' Mot. at 6 nn. 5–8. But in those paragraphs of Mr. Klein's declaration, he does not describe the contents and purpose of the SG3 Secure Room. Rather, he focuses on his work elsewhere with a splitter cabinet that he states diverted copies of certain signals into that room. *See* Klein Decl. ¶¶ 24–34. As to what, if anything, happened to those signals once inside the room—the key information that Plaintiffs' evidence must establish—Mr. Klein is silent except to point to Exhibit C to his declaration, [redacted] which purportedly includes a list of equipment to be

installed in the SG3 Secure Room. *Id.* ¶ 35 & Exh. C at 3-[redacted]

[redacted]

Notably, while Plaintiffs defend much of the Klein declaration as "within his personal knowledge," they exclude his testimony regarding the SG3 Secure Room from that argument. *See* Pls.' Opp. at 25–27. Rather, they claim that Klein's testimony regarding the devices in the SG3 Secure Room "is based on the AT&T documents he relied on to do his job." *Id.* at 29. The declaration does not support that claim. As to Exhibit C, the document in question, Mr. Klein states only (and ambiguously) that "[i]n the course of [his] employment, [he] reviewed [it];" he does not attest that the equipment listed in the document was in fact installed in the SG3 Secure Room. Klein Decl. ¶ 28. Based on his own statements, Mr. Klein did not work in or, except on one brief occasion, ever set foot in the SG3 Secure Room, *id.*¶ 17, and he is not competent to offer evidence of the equipment actually installed there, much less the purpose of that equipment.

[redacted]

Likewise, Mr. Marcus does not claim personal knowledge or provide other competent evidence regarding the equipment in the SG3 Secure Room or its purpose. He simply assumes the equipment in Klein Exhibit C was in fact installed there. Plaintiffs nonetheless urge the Court to rely on his testimony because, under Rule 703, a witness proffered as an expert "is not limited to his personal knowledge and can rely on the testimony and evidence of others . . . that would themselves be inadmissible." Pls.' Opp. at 30. But Plaintiffs ignore that "[t]he fact that inadmissible evidence is the (permissible) premise of [an] expert's opinion does not make that evidence admissible for other purposes, purposes independent of the opinion." *In re James Wilson Assocs.*, 965 F.2d 160, 173 (7th Cir. 1992); *see also* Wigmore Evid. § 4.7.2. Thus, Rule 703 does not permit Mr. Marcus's purported expertise to transform hearsay and speculation into admissible evidence about what was actually installed (or occurred) in the SG3 Secure Room. On the contrary, because Mr. Marcus's proffered opinions are not "based on sufficient facts or data" as required by Rule 702(b), those opinions are inadmissible too. *See* Gov't Mem. at 17–18.

In sum, Plaintiffs offer no admissible evidence regarding the equipment actually installed in the SG3 Secure Room, or, more importantly, the purpose of that equipment.[2] Plaintiffs, therefore, have adduced no competent evidence that their communications were collected for purposes of surveillance, even in 2003-04. Their claim should be rejected on that basis alone.

B. Plaintiffs Have Presented No Competent Evidence of NSA Involvement in Activities Conducted in the SG3 Secure Room.

Similarly, neither the Klein nor the Marcus declaration provides admissible evidence of Government involvement in the SG3 Secure Room. For all of the reasons explained in the Government's cross-motion, Mr. Marcus's testimony that it is "plausible" the Government funded the room does not pass muster under Rule 702; he lacks both expertise in corporate finance and a factual foundation for the conclusions he offers, *see* Gov't Mem. at 16–18.

Nor can Mr. Klein's testimony establish Government involvement here. Plaintiffs now claim that Mr. Klein saw an AT&T management technician who had met with an NSA agent installing equipment in the SG3 Secure Room, *see* Pls.' Opp. at 27, and that AT&T management sent an email establishing AT&T's intention to work with NSA, *see id.* at 28. Mr. Klein's declaration does not support either statement. Mr. Klein does not state that he observed a management technician installing equipment in the SG3 Secure Room as Plaintiffs claim, *see* Pls.' Opp. at 27; rather, he notes that he saw "a workman apparently working on the door lock for the room." Klein Decl. ¶ 12. So, too, with the email that Mr. Klein mentions. He states that management sent an email regarding "the pending visit" and that the email "explicitly mentioned the NSA." *Id.* ¶ 10. Based on Mr. Klein's two-year-old recollection of that scant text, Plaintiffs urge the Court to find that two separate meetings occurred between AT&T and NSA, infer a resulting agreement between AT&T and NSA to work together, and conclude that "AT&T thereafter did cooperate with the NSA." Pls' Opp. at 28. There is no basis in Mr. Klein's declaration—or, indeed, in common sense—for these sweeping conclusions.

Similarly, although Plaintiffs claim that Mr. Klein knew that only personnel cleared by NSA could access the SG3 Secure Room "based on [his] personal knowledge, observations, and

[2] Plaintiffs' proffered evidence is even less probative of what, if any, activity occurred at other AT&T facilities where Mr. Klein claims "[he] learned that other . . . 'splitter cabinets' were being installed." Klein Decl. ¶ 36.

experiences of AT&T's business operations and its policies and practices," Pls.' Opp. at 27, no such assertions appear in Mr. Klein's declaration. Indeed, Plaintiffs do not even cite to the declaration as support for that claim. *See id.* Where Mr. Klein's declaration specifically discusses the claimed NSA restriction on access to the SG3 Secure Room, he qualifies it with the disclaimer "[t]o my knowledge," Klein Decl. ¶ 17, and goes on to discuss the limitations on that knowledge, *see id.* (noting that he had no access to the SG3 Secure Room). In reality, Mr. Klein makes clear that his testimony is based on hearsay. *See, e.g., id.* ¶ 16 ("FSS# 1 told me that another NSA agent would again visit . . ."). And while Plaintiffs argue that "statements made to Klein by management and other AT&T employees about NSA's activities . . . are admissible nonhearsay" because AT&T is the Government's "agent" and "co-conspirator," Pls.' Opp. at 28, these arguments assume the very conclusions Plaintiffs are trying to prove. Plaintiffs ask the Court to assume a relationship exists to facilitate the admission of the very statements that Plaintiffs claim establish the relationship. The Court should reject such circular reasoning.[3]

C. Plaintiffs Have Presented No Competent Evidence of Ongoing Activity at the Folsom Street Facility, or Elsewhere, to Support Their Claims.

Most importantly, Plaintiffs' claim of "ongoing seizures and searches," Pls.' Mot. at 1, rests wholly on stale "evidence" of activities occurring over ten years ago, five years before Section 702 was enacted, and has no probative value regarding the scope, sources, or methods of Upstream collection today. Plaintiffs maintain—without citation to any authority—that there is no "freshness" rule of evidence, Pls.' Opp. at 31, but to the contrary, before evidence may be admitted as relevant, it must be probative of the matter before the Court, and on this basis courts routinely exclude evidence that is too remote in time.[4] As the Ninth Circuit held in *Ortega v.*

[3] In support of their agency theory, Plaintiffs cite AT&T's 2014 Transparency Report as an admission that "AT&T conducts surveillance for the NSA under the [FISA]." *See* Pls.' Opp. at 24. But the timeframe covered by the report—July 1–December 31, 2013—is irrelevant to whether the Government was in any way involved in the alleged activity in the SG3 Secure Room over ten years ago. At best the report reveals in general that AT&T recently responded to national security demands under FISA from unidentified Government agencies, and not whether AT&T did or did not participate in any particular form of collection (such as Upstream, PRISM, or traditional FISA orders) at the behest of any particular agency.

[4] *See* Fed. R. Evid. 401; *see, e.g., Wilson v. Bradlees of New England, Inc.*, 250 F.3d 10 (1st Cir. 2001) (affirming exclusion and restriction of "stale hearsay" and other unduly prejudicial material); *Chertkova v. Connecticut Gen. Life Ins. Co.*, 210 F.3d 354 (Table), 2000 WL 349277, at *4 (2d Cir. Apr. 4, 2000) (affirming exclusion "as too distant, evidence of events

O'Connor, 146 F.3d 1149, 1162 (9th Cir. 1998), evidence of events occurring over ten years ago is too stale even to meet a requirement of reasonable suspicion, much less to prove by a preponderance of the evidence that conduct of which a litigant complains remains ongoing. *See also Herrera v. Perry*, 2014 WL 2557644, at *8 (C.D. Cal. Mar. 19, 2014) (denying preliminary injunction where plaintiff "[had] not presented any evidence that [alleged] tampering [and] fabricating evidence over ten years ago remain on-going").[5]

The only contemporary evidence that Plaintiffs cite is the Government's acknowledgment that Upstream collection of communications from the Internet backbone is "active and ongoing." *See* Pls' Opp. at 31. But that general acknowledgment does not establish that collection occurs at Folsom Street, that Plaintiffs' communications are included, or that the means employed actually resemble the four-stage process Plaintiffs describe—either now, or at any time in the past. For lack of evidence to support Plaintiffs' Fourth Amendment claim, or their standing to raise it, the Court should grant the Government's cross-motion for summary judgment.[6]

---

that had allegedly occurred 11 years before the relevant period"); *Perry v. Ethan Allen, Inc.*, 115 F.3d 143, 150 (2d Cir. 1997) (affirming exclusion of events more than six months prior to alleged harassment as "too remote to have probative value"); *Bhasin v. Bluefield Regional Med. Ctr., Inc.*, 62 F.3d 1414 (Table), 1995 WL 465796, at *4 (4th Cir. Aug. 8, 1995) (affirming exclusion of events from early 1980s as "too remote" from a discharge in 1992); *West v. Drury Co.*, 2009 WL 1532491, at *1 (N.D. Miss. 2009) (excluding medical record more than a decade old); *Sanchez v. Echo, Inc.*, 2008 WL 2951339, *4 (E.D. Pa. Jan. 9, 2008); *Dimas v. Michigan Dep't of Civil Rights*, 2004 WL 1397558, at *12, n.2 (W.D. Mich. Mar. 19, 2004) (excluding statements ten years prior to alleged discrimination as "too remote in time . . . to be probative").

[5] Indeed, even if the Klein and Marcus declarations eked past the threshold of relevance, Plaintiffs' burden is still to present a quantum of evidence on which a reasonable trier of fact could find that the surveillance activities they allege are ongoing, *and* that they include Plaintiffs' communications. *See In re Oracle Corp. Sec. Litig.*, 627 F.3d 376, 387 (9th Cir. 2010). Speculation regarding events occurring over ten years ago is at best a mere "scintilla of evidence in support of the [P]laintiff's position," and as such is "insufficient" to avoid summary judgment. *United States v. $133,420 in U.S. Currency*, 672 F.3d 629, 638 (9th Cir. 2012).

[6] Plaintiffs contend that even if the proffered evidence does not meet their burden, the Court cannot grant summary judgment for the Government because they are "entitled" to pursue discovery. Pls.' Opp. at 35, citing Fed. R. Civ. P. 56(d). To be entitled to Rule 56(d) discovery, parties must establish (1) that they have "set forth in affidavit form the specific facts [that they] hope[] to elicit from further discovery; (2) [that] the facts sought exist; and (3) [that these] sought-after facts are 'essential' to oppose summary judgment." *Family Home & Fin. Ctr., Inc. v. FHLMC*, 525 F.3d 822, 827 (9th Cir. 2008). The facts sought "must be based on more than mere speculation." *SW Traders LLC v. United Specialty Ins. Co.*, 409 Fed. Appx. 96, 98–99 (9th Cir. 2010). Here, Plaintiffs cite to two affidavits previously submitted in this litigation, *see* Pls.' Opp. at 35 (citing ECF Nos. 30, 114), but they do not fulfill Rule 56(d)'s requirements. Both declarations list sweeping categories of discovery, *see* ECF No. 30 ¶¶ 7, 11, 12; ECF No. 114 ¶¶ 7, 11, 12, but fail to state the particular facts they hope to prove or to establish that the facts exist, offering only such generalities as "the discovery would lead to evidence regarding the nature and

II. PLAINTIFFS' CLAIMS OF FOURTH AMENDMENT SEARCHES AND SEIZURES ALSO FAIL AS A MATTER OF LAW.

A. In Addition to the Lack of Supporting Evidence, Plaintiffs Offer No Legal Support for Their "Stage 1" Seizure Claim.

Plaintiffs likewise offer no legal support for their claim that the alleged (but unproven) copying of online communications at Stage 1 of the Upstream process constitutes a Fourth Amendment seizure. *See* Gov't Mem. at 23-30. Exclusively at issue here are copies of communications that in Plaintiffs' telling are electronically created at Stage 1, scanned for targeted selectors at Stage 3, and then, because they are found to contain no such selectors, are destroyed, all within milliseconds of their creation. *See* Gov't Mem. at 28-29; Pls.' Mot. at 9. Plaintiffs now assert that Upstream collection interferes with a right to "sole possession" and "exclusive control" of the information these communications contain. Pls.' Opp. at 3, 4. But they still have not explained how the alleged creation and destruction of copied communications within milliseconds "meaningful[ly] interfere[s]" with such an interest, so as to constitute a Fourth Amendment seizure. *See United States v. Jacobsen*, 466 U.S. 109, 113 (1984).

Plaintiffs maintain that the "act of copying" itself effects a seizure "the moment" the copies are made, regardless of how long they are kept, by interfering with this "right to [exclusive] control." Pls.' Opp. at 4-6. This concept of a seizure ignores the requirement that interference with a possessory interest in property be meaningful, and the Ninth Circuit has rejected the proposition, upon which Plaintiffs' argument depends, "that *any* detention of [property] constitutes a fourth amendment seizure." *United States v. England*, 971 F.2d 419, 421 (9th Cir. 1992); *see also United States v. Jefferson*, 566 F.3d 928, 933-34 (9th Cir. 2009) (rejecting contention that possessory interest in package arose at the time it was removed from the mail stream); *United States v. Hoang*, 486 F.3d 1156, 1160-62 (9th Cir. 2007) (similar). As explained in *United States v. Va Lerie*, 424 F.3d 694, 706 (8th Cir. 2005) (en banc):

> [N]ot all police interference with an individual's property constitutes a Fourth Amendment seizure, i.e., the police do not seize property every time they handle private property. By requiring some *meaningful interference* with an individual's possessory interests in property, the Supreme Court inevitably contemplated excluding *inconsequential interference* with an individual's possessory interests.

---

scope of the Government's surveillance program." *Id.* ¶ 20. Such conclusory statements do not provide the specific showing required under Rule 56(d).

Applying these principles, the courts, including the Ninth Circuit, have refused to find Fourth Amendment seizures where detentions of property lasting much longer than those alleged here resulted in no consequential interference with the owners' possessory interests.[7] These cases, and those previously cited by the Government involving the momentary handling of property for brief non-intrusive inspections, *see* Gov't Mem. at 27, dispel the notion that the alleged "act of copying" communications itself constitutes a seizure "the moment" it occurs.

Plaintiffs attempt to dismiss this body of precedent on the basis that the cases "do not speak to [interference with] the possessory interest in the contents of [] communication[s]," Pls.' Opp. at 7, but they do not explain the supposed import of this distinction. These cases illustrate the principle, announced in *Jacobsen*, that interference with a possessory interest must be meaningful *before* a seizure can take place. Under this principle as elaborated in the case law, no such interference with a right of exclusive control over the content of communications has been shown merely from the alleged act of copying them, where, in Plaintiffs' own telling, the copies are destroyed within milliseconds.

Plaintiffs cite *United States v. Place*, 462 U.S. 696 (1983) for the proposition that even a brief detention of property can result in a seizure, Pls.' Opp. at 6, but in contrast to the initial 90-minute detention of the traveler's luggage in *Place*, *id.* at 709, the lifetime of the copied communications here is vanishingly brief, and involves none of the circumstances or ensuing consequences that *Place* considered, and that the Ninth Circuit and other courts look to, in determining whether a seizure has occurred: no property is taken from anyone's immediate possession; no property is destroyed; delivery of no one's communications is delayed; and no one's freedom of movement is impeded.[8] Once the allegedly copied communications are scanned and destroyed, all within milliseconds of their creation, "exclusive" control over the

[7] *See, e.g.*, *United States v. Clutter*, 674 F.3d 980, 983-85 (8th Cir. 2012) (detention of defendant's home computers after he had been jailed); *Jefferson*, 566 F.3d at 931-35 (overnight detention of express mail); *Hoang*, 486 F.3d at 1158, 1160-62 (ten-minute detention of FedEx package); *United States v. Gant*, 112 F.3d 239, 240, 242 (6th Cir. 1997) (moving passenger's tote bag from overhead bin to seat for narcotics "sweep" of bus by drug-sniffing dog).

[8] *See Jacobsen*, 466 U.S. at 124-25; *Clutter*, 674 F.3d at 984-85; *Jefferson*, 566 F.3d at 934-35; *Hoang*, 486 F.3d at 1160; *Va Lerie*, 424 F.3d at 703-07; *Gant*, 112 F.3d at 242; *United States v. Brown*, 884 F.2d 1309, 1311 (9th Cir. 1989); *United States v. Beale*, 736 F.2d 1289, 1289-90, 1292 (9th Cir. 1984). *See also Place*, 462 U.S. at 718 n.5 (Brennan, J., concurring).

communications is restored to the parties as if the copies allegedly obtained by the Government had never been created at all.[9]

For their part, Plaintiffs cite no authority for the proposition that the "act of copying" a communication results in a seizure "the moment it occurs." To a one, the cases Plaintiffs cite in support of this assertion involved situations where government agents not only copied or recorded the contents of oral or electronic communications, but also retained those copied communications indefinitely, in some cases for months and years at a time, and used the contents for their own investigative or prosecutorial purposes.[10] The Government has already explained, however, that the allegations here are distinguishable from the circumstances of such precedents, because they concern copies of communications that are not retained or put to any use by the Government, and instead are destroyed instantaneously after their creation once it is determined (by electronic means) that they do not contain targeted selectors. *See* Gov't Mem. at 28-29. Plaintiffs do not cite a single case in which the copying of digital information alone, without retention, was held to be a seizure.[11] Plaintiffs warn that "[u]nder the [G]overnment's argument, digital information would never be considered 'seized' unless [it] [also] took possession of … a

[9] In holding that no seizure occurs when government agents briefly handle or detain a piece of mail or stowed luggage, courts have further observed that persons who place items in the mail, or check baggage with a carrier, have no reasonable expectation that those items will not be touched, handled, or moved around by strangers en route to their destination. *United States v. Terriques*, 319 F.3d 1051, 1055 (8th Cir. 2003); *United States v. DeMoss*, 279 F.3d 632, 635 (8th Cir. 2002); *see also Jacobsen*, 466 U.S. at 113. Likewise, Plaintiffs can have no reasonable expectation that intermediate copies of their communications will not be made (and for some period stored) by numerous computers as they make their way across the Internet, *see, e.g.*, *United States v. Councilman*, 418 F.3d 67, 69-70 (1st Cir. 2005), or that copies of the communications will not continue to reside on faraway, even overseas servers of the providers to which the parties to Plaintiffs' communications subscribe. *See In re Warrant to Search a Certain E-Mail Account*, 2014 WL 1661004, at *4 (S.D.N.Y. Apr. 25, 2014).

[10] *See Katz v. United States*, 389 U.S. 347, 348 (1967); *Berger v. State of New York*, 388 U.S. 41, 45 (1967); *United States v. Ganias*, 755 F.3d 125, 128-30, 137 (2d Cir. 2014); *United States v. Comprehensive Drug Testing, Inc.*, 513 F.3d 1085, 1093 (9th Cir. 2008), *aff'd en banc,* 621 F.3d 1162 (9th Cir. 2010); *In re Search of Info. Associated with [Redacted]@mac.com*, 2014 WL 1377793, at *2 (D.D.C. Apr. 7, 2014). *See also LeClair v. Hart*, 800 F.2d 692, 693 (7th Cir. 1986); *United States v. Jefferson*, 571 F. Supp. 2d 696, 699-700, 703 (E.D. Va. 2008).

[11] Plaintiffs are also unaided by cases holding that a prohibited acquisition of electronic communications occurs under the Wiretap Act, 18 U.S.C. § 2511(a), "when the contents of a wire communication are captured or redirected in any way." Pls.' Opp. at 5. Statutory enactments can satisfy the requirements of the Fourth Amendment, but do not affect the scope of the protections it affords. *See United States v. Mann*, 829 F.2d 849, 851-53 (9th Cir. 1987); *United States v. Kington*, 801 F.2d 733, 737 (5th Cir. 1986).

hard drive or a server" containing the data. Pls.' Opp. at 5. But again they miss the point. The critical distinction is not whether the Government obtains communications by electronically copying them or seizing the hardware on which they reside, but whether the Government's retention of the data is of such duration, or results in other consequences, as to meaningfully interfere with the owner's possessory interests. Plaintiffs have made no such showing here.[12]

B. Plaintiffs Also Offer No Legal Support for Their "Stage 3" Search Claim.

The Government has shown that, under the reasoning of *Place* and *Jacobsen*, electronic scanning of copied communications that occurs at Stage 3 of the alleged Upstream process does not constitute a search of the only communications that Plaintiffs have placed at issue here: those not found to contain targeted selectors, which are immediately destroyed, not retained by the Government. Because under Plaintiffs' scenario Government agents obtain no information about the communications, their contents, the parties to them, or even that they exist, the alleged electronic scanning of those communications for targeted selectors "does not compromise any legitimate interest in privacy." *Jacobsen*, 466 U.S. at 122-23; *see* Gov't Mem. at 31-33.

Plaintiffs contest the point that no search occurs if no information is actually provided to Government agents. Pls.' Opp. at 9, 11. But in so doing they take issue with first principles, *see Florida v. Jardines*, 133 S. Ct. 1409, 1414 (2013) ("exclusive basis" for invoking Fourth Amendment's protections against unreasonable searches requires that the "Government obtain[ ] information"), and the rationale of *Place*, 462 U.S. at 707 (canine sniff of luggage for narcotics is not a search because it does not otherwise expose the contents of the luggage to Government agents), as extended in *Jacobsen*, 466 U.S. at 123-24. And contrary to Plaintiffs' contention that "[t]he [G]overnment's human-eyes thesis is … unsupported by authority," Pls.' Opp. at 9, the distinction between electronically scanning digital information for data of interest and actually revealing that information to human beings is recognized by courts, Congress, commentators,

[12] Plaintiffs again conflate possessory and privacy interests when they argue that the alleged Stage 1 copying of communications is "intrusive" because, no matter how briefly the copies are retained, they are scanned in the interim (at Stage 3) for targeted selectors. Pls.' Opp. at 7; *see* Gov't Mem. at 30 n.7. Courts have held repeatedly that it does not matter to the seizure inquiry that government agents briefly handle, detain, or divert an object for the purpose of gleaning information through some non-invasive technique. *See, e.g.*, *Arizona v. Hicks*, 480 U.S. 321, 324-25 (1987); *Jefferson*, 566 F.3d at 931-32, 934-35; *DeMoss*, 279 F.3d at 634, 635-36; *Gant*, 112 F.3d at 240, 242; *United States v. Hall*, 978 F.2d 616, 618-20 (10th Cir. 1992).

and other legal authorities.[13] It is also supported by the Supreme Court's decision in *United States v. Karo*, 468 U.S. 705, 712-13 (1984) (placement of an unmonitored tracking device among suspect's belongings did not infringe upon his privacy because until monitored by Government agents the device "conveyed no information at all").

Plaintiffs next argue that the holdings of *Place* and *Jacobsen* do not apply to investigative techniques that can reveal something other than the presence or absence of contraband, Pls.' Opp. at 10-11, but once again they fail to grapple with the issue at hand. *Jacobsen* teaches that the critical question in each case involving an alleged search is whether "[o]fficial conduct … 'compromise[d] any legitimate interest in privacy.'" *See Illinois v. Caballes*, 543 U.S. 405, 408 (2005), quoting *Jacobsen*, 466 U.S. at 123. Here, the alleged automated scanning of communications that are not found to contain targeted selectors reveals no information about them, not even the fact of their existence, and is thus designed, like the chemical test in *Jacobsen*, so that "it could reveal nothing" about non-targeted communications. *Jacobsen*,466 U.S. at 124 n.24; *see* Gov't Mem. at 33. So far as these communications are concerned, Stage 3 scanning for selectors "does not expose" anything about them "that otherwise would remain hidden from public view." *Place*, 462 U.S. at 707. Hence, the "official conduct" alleged in this proceeding involves no search under the Fourth Amendment.[14]

---

[13] *See In re Warrant to Search a Certain E-Mail Account, supra*, 2014 WL 1661004, at *6; S. Rep. No. 99-541, 99th Cong., 2d Sess. 20 (1986) ("monitor[ing] a stream of transmissions in order to properly route, terminate, and otherwise manage the individual messages" is not prohibited by the Wiretap Act because "[t]hese monitoring functions . . . do not involve humans listening in on voice conversations"); Bruce E. Boyden, Can a Computer Intercept Your Email?, 34 Cardozo L. Rev. 669, 673 (2012) (arguing that "automated processing [of e-mail] that is not contemporaneously reviewable by . . . humans, and does not produce a record for later human review, is not an interception [under] the Wiretap Act"); Richard A. Posner, Privacy, Surveillance, and Law, 75 U. Chi. L. Rev. 245, 254 (2008) ("Computer searches do not invade privacy because search programs are not sentient beings. Only [a] human search should raise constitutional or other legal issues."); Orin S. Kerr, Searches and Seizures in a Digital World, 119 Harv. L. Rev. 531, 547-48, 551-54 (2005) (contending that "a search of data stored on a hard drive occurs when that data … is exposed to human observation"); Use of E-Mail Service Provider That Scans E-Mails For Advertising Purposes, NY Eth. Op. 820 (2008) (a lawyer may use an e-mail service provider that conducts computer scans of e-mails to generate computer advertising, without breaching client confidentiality, where the e-mails are not reviewed by or provided to human beings other than the sender and recipient); Legal Ethics, Law. Deskbk. Prof. Resp. § 1.6-2(c) (2013-2014 ed.) ("general rule" same).

[14] Plaintiffs cite no authority to support their contrary view. *See* Pls.' Opp. at 12-13. As a result of the "hash value" analysis conducted on the defendant's computer in *United States v. Crist*, 627 F. Supp. 2d 575, 578 (M.D. Pa. 2008), law-enforcement agents actually obtained

Whether scanning communications that are found to contain targeted selectors (and are therefore retained) infringes upon a legitimate expectation of privacy is not at issue here.[15] Plaintiffs, having identified no communications of their own that fall into that category, have excluded it from the ambit of their summary judgment motion, Pls.' Mot. at 9, and cannot "vicariously assert[ ]" the Fourth Amendment rights of persons whose communications are found to contain targeted selectors to support their very different claim. *Rakas v. Illinois*, 439 U.S. 128, 133-34 (1978); *United States v. Pulliam*, 405 F.3d 782, 789-90 & n.3 (9th Cir. 2005). The only question that is or can be presented by Plaintiffs' motion is whether they have shown a violation of their own Fourth Amendment rights, and as a matter of law (as well as fact), the answer is no.

All else failing, Plaintiffs warn that failure to adopt their view of the Fourth Amendment will license "a digital surveillance state," Pls.' Opp. at 9, albeit a peculiar one in which the state avoids collecting information about the vast majority of the millions of people upon whom it supposedly spies. The Supreme Court has repeatedly refused in the past to accept such dire predictions as a substitute for application of settled constitutional principles, *see, e.g., United States v. Knotts*, 460 U.S. 276, 283-84 (1983), and there is no reason to indulge them in the circumstances here.[16] Plaintiffs have not demonstrated that Upstream collection involves searches (or seizures) that violate their Fourth Amendment rights.

---

information from which they were able to glean the contents of over 170 files on the computer. *Bourgeois v. Peters*, 387 F.3d 1303, 1307, 1314 n.9 (11th Cir. 2004), was an action to enjoin mass magnetometer screening at an outdoor political protest, including physical searches of individuals and their belongings in instances when the magnetometers revealed the presence of metal on their persons. (It was not disputed that the magnetometer screening constituted a search.) In contrast, Plaintiffs' claim here does not encompass those instances where Stage 3 scanning of communications reveals the presence of targeted selectors.

[15] Hence, the Government's position here does *not* turn on whether communications that contain targeted selectors may be considered "contraband." *See* Pls.' Opp. at 11.

[16] For foreign intelligence purposes, FISA already prohibits "electronic surveillance and the interception of domestic wire, oral, or electronic communications" except as the statute itself allows. 50 U.S.C. § 1812(a). (Electronic surveillance for federal law enforcement purposes is regulated by Title III of the Omnibus Crime Control and Safe Streets Act, 18 U.S.C. §§ 2510-2520, *see United States v. U.S. Dist. Court (Keith)*, 407 U.S. 297, 302 (1972).) Section 702, in particular, "create[s] a comprehensive scheme in which the [FISC] evaluates the Government's certifications, targeting procedures, and minimization procedures" to ensure that they meet statutory requirements, and "comport with the Fourth Amendment." *Clapper v. Amnesty Int'l*, 133 S. Ct. 1138, 1154 (2013) (citing 50 U.S.C. § 1881a(a), (c)(1), (i)(2)-(3)). Congress oversees the Government's exercise of its Section 702 authority, 50 U.S.C. §§ 1871, 1881a(l), 1881f, and has demonstrated its willingness and ability, both in enacting FISA and otherwise, to legislatively "balance privacy and public safety in a comprehensive way," *United States v. Jones*,

III. UPSTREAM COLLECTION IS REASONABLE UNDER THE SPECIAL NEEDS DOCTRINE.

The Government demonstrated in its opening brief that even if the alleged real-time electronic copying and scanning of online communications constitute seizures and searches under the Fourth Amendment, these activities are constitutional under Fourth Amendment "special needs" analysis because (1) temporarily creating copies of online communications and electronically scanning them for targeted selectors, followed by their immediate destruction, at most minimally intrudes on Fourth Amendment interests, and (2) Upstream collection of foreign intelligence makes significant contributions to national security. Gov't Mem. at 34-43.

Plaintiffs' responses are unavailing. They argue first that warrantless searches have only been upheld under the special needs doctrine where the persons searched had diminished expectations of privacy due to their choice to engage in certain regulated activities, and second that no similar special needs case involves seizures and searches on such a scale as allegedly occurs under Upstream collection. Pls.' Opp. at 15-16. These arguments misstate the Supreme Court's special needs jurisprudence. "The special needs doctrine does not require that the subject of the search possess a diminished privacy interest." *MacWade v. Kelly*, 460 F.3d 260, 269 (2d Cir. 2006). *See also United States v. Aukai*, 497 F.3d 955, 960 (9th Cir. 2007) (en banc) ("The constitutionality of an airport screening search . . . does not depend on consent."). While many of the Court's special needs cases have involved diminished privacy expectations, "the Supreme Court never has implied—much less actually held—that a reduced privacy expectation is a *sine qua non* of special needs analysis," *MacWade*, 460 F.3d at 269, and the Court has in fact applied special needs analysis where individual expectations of privacy were undiminished. *See, e.g.*, *Camara v. Municipal Court*, 387 U.S. 523, 537 (1967) (routine building inspections for health-code compliance); *Michigan Dep't of State Police v. Sitz*, 496 U.S. 444 (1990) (warrantless traffic checkpoints to screen for intoxicated drivers); *United States v. Martinez-*

---

132 S. Ct. 945, 964 (2012) (Alito J., concurring). *See Keith*, 407 U.S. at 302; *United States v. Frazin*, 780 F.2d 1461, 1465 (9th Cir. 1986) (noting Congress enacted the Right to Financial Privacy Act in response to the holding of *United States v. Miller*, 425 U.S. 435 (1976), that bank customers have no legitimate expectation of privacy in bank records). The criminal justice system also provides a forum for persons whose communications are actually acquired (and used against them) to place the exercise of the Government's Section 702 authority under judicial scrutiny. *See United States v. Mohamud*, 2014 WL 2866749, at *15-18 (D. Or. June 24, 2014).

Fuerte, 428 U.S. 543 (1976) (same to screen for illegal aliens). *See also Al-Haramain Islamic Found., Inc. v. U.S. Dep't of the Treasury*, 686 F.3d 965, 991-92 (9th Cir. 2012) (discussing these as "major" special needs cases).

To be sure, the Supreme Court has explained that in cases involving "substantial expectations of privacy" the special needs test requires the program to serve "some purpose other than 'to detect evidence of ordinary criminal wrongdoing.'" *Maryland v. King*, 133 S. Ct. 1958, 1978 (2013) (quoting *Indianapolis v. Edmond*, 531 U.S. 32, 38 (2000)). Significantly, Plaintiffs acknowledge that "a significant purpose" of Upstream collection under Section 702 is to obtain foreign intelligence. Pls.' Opp. at 16-17. Thus, contrary to Plaintiffs' argument, Upstream collection fits comfortably within the special needs doctrine because its undisputed programmatic purpose exceeds normal law enforcement needs. Nor is the scale of the seizures and searches alleged here unprecedented in special needs cases. *See Aukai*, 497 F.3d at 956, 958-62 (applying the special needs analysis to uphold warrantless screening by TSA of all commercial aircraft passengers—some 700 million people each year).

Plaintiffs next take issue with the Government's demonstration that it is impracticable to obtain a warrant based on probable cause every time it seeks to collect intelligence targeting non-U.S. persons outside the United States, arguing that the Congressional committee reports cited by the Government in support of this conclusion are inadmissible hearsay and not specific to Upstream collection. Pls.' Opp. at 18. Significantly, Plaintiffs do not challenge Congress's determination, reflected in the reports and the enactment of Section 702, that having to obtain individual FISA warrants to collect this type of intelligence, merely as an unintended result of changes in technology, seriously burdened the Government's intelligence resources and impeded its collection of foreign intelligence; and that authorization of surveillance under the terms and conditions of Section 702 substantially improved the Government's ability to quickly and effectively monitor terrorist communications. *See, e.g.*, H.R. Rep. No. 112-645(II) at 2-3; *id.* (I) at 4; S. Rep. No. 112-174 at 2; S. Rep. No. 110-209 at 5; May 1, 2007 FISA Mod. Hrg. at 18; Gov't Mem. at 4-5. Plaintiffs' attempts to diminish the force of these conclusions on hearsay and specificity grounds are entirely without merit.

The Congressional reports cited by the Government are admissible under Federal Rule of Evidence 803(8), which provides that a public record or statement setting forth factual findings from a legally authorized investigation is not excluded as hearsay if "neither the source of information nor other circumstances indicate a lack of trustworthiness." *See also Beech Aircraft Corp. v. Rainey*, 488 U.S. 153, 162, 170 (1988) (factually based conclusions or opinions admissible too, if trustworthy). Public records are presumed trustworthy, and the burden of establishing a basis for excluding a public record falls on the party opposing the evidence. *Gilbrook v. City of Westminster*, 177 F.3d 839, 858 (9th Cir. 1999); *Johnson v. City of Pleasanton*, 982 F.2d 350, 352 (9th Cir. 1992). Courts look to four factors in assessing a public report's trustworthiness: (1) the timeliness of the investigation; (2) the special skill or expertise of the investigating official; (3) whether a hearing was held and the level at which it was conducted; and (4) possible motivation problems. *Beech Aircraft*, 488 U.S. at 167 n.11; *Barry v. Trustees of the Int'l Ass'n Full-Time Salaried Officers & Employees of Outside Local Unions & Dist. Counsel's (Iron Workers) Pension Plan*, 467 F. Supp. 2d 91, 97 (D.D.C. 2006). Courts also ask whether findings and conclusions in Congressional reports are the product of serious investigation rather than political grandstanding, and whether members of the minority party dissented from the report. *Barry*, 467 F. Supp. 2d at 98-100 (discussing cases).

The sum total of Plaintiffs' argument on this front is to declare that the Congressional statements relied on to demonstrate impracticability (and Upstream's effectiveness), are "inadmissible hearsay," citing to Fed. R. Evid. 801(c), 802. Pls.' Opp. at 18, 23. Plaintiffs have "produced no evidence [or even argument] whatsoever to raise doubts about the reliability" of these Congressional statements, nor challenged the motives of the reporting committees. *Gilbrook*, 177 F.3d at 858. *See also Johnson*, 982 F.2d at 353. This is no surprise, as the factors noted above all point in favor of the reports' reliability, and, therefore, admissibility.

The statements cited by the Government are contained in timely reports on the FISA Amendments Act ("FAA"), *see* S. Rep. No. 110-209, and the reauthorization of the FAA (which would have expired at the end of the year in which those reports were issued). *See* H.R. Rep. No. 112-645(II) at 2. The issuing committees—the House and Senate Select Committees on

Intelligence and Committees on the Judiciary—all had expertise in the subject of the collection of foreign intelligence under the FISA and the FAA. *See*, *e.g.*, S. Rep. No. 112-174 at 2, 7; S. Rep. No. 110-209 at 1; H.R. Rep. No. 112-645(II) at 3-4. In addition, the committees held hearings and briefings on the issues discussed in the reports. *See* H.R. Rep. No. 112-645(I) at 3-4; H.R. Rep. No. 112-645(II) at 4-6; S. Rep. 112-229 at 9; S. Rep. No. 112-174 at 2; S. Rep. No. 110-209 at 2. Finally, there is no suggestion that the reports' conclusions are the product of improper motives or grandstanding; they reflect serious bipartisan consideration of important national security issues, with little minority dissent (principally related to issues of privacy, transparency, and oversight for which the Government did not cite the reports). *See* H.R. Rep. No. 112-645(II) at 10-11; H.R. Rep. No. 112-645(I) at 17-21; S. Rep. No. 112-174 at 10-12; *but see* S. Rep. No. 112-229 at 15-16. Other FAA legislative history cited by the Government, such as the 2007 FISA Modernization Hearing, has been cited by other courts, *see Mohamud*, 2014 WL 2866749, at * 7-8, indicating its reliability as well. *See Sobel v. Hertz Corp.*, 291 F.R.D. 525, 533 (D. Nev. 2013). Thus, the Congressional reports relied upon by the Government are admissible under Fed. R. Evid. 803(8). *See, e.g.*, *Barry*, 467 F. Supp. 2d at 99-101; *Mariani v. United States*, 80 F. Supp. 2d 352, 358-61 (M.D. Pa. 1999); *Gathercole v. Global Assocs.*, 560 F. Supp. 642, 647 (N.D. Cal. 1983); *Hobson v. Wilson*, 556 F. Supp. 1157, 1181 (D.D.C. 1982).[17]

Plaintiffs' further argument that the public reports cited by the Government should be disregarded because they are not specific to Upstream collection is also meritless. Congress's determination that it is impracticable to obtain individual warrants for purposes of foreign intelligence collection targeted at non-U.S. persons does not turn on which method the Government uses instead to collect such intelligence. Because of changes in technology, the Government was required under FISA to obtain judicial authorization to collect the communications of non-U.S. persons located outside the U.S. (a result not intended by FISA's original authors, *see* Gov't Mem. at 4-5), "significantly divert[ing] NSA analysts from their

[17] The Privacy & Civil Liberties Oversight Bd. Report on the Surveillance Program Operated Pursuant to Section 702 of the FISA, and the report of The President's Review Group on Intelligence and Communications Technologies, Liberty and Security in a Changing World (Dec. 12, 2013) —both of which Plaintiffs themselves cite (Pls.' Opp. at 17-18, 24 n.16; Pls.' Mot. at 4 n.3, 7 n.10, 8 n.12-13, 9 & n.14, 22, 25 n.24)—are likewise trustworthy.

counterterrorism mission" and "degrad[ing] capabilities in the face of a heightened terrorist threat environment." S. Rep. No. 110-209 at 5; *see also* May 1, 2007 FISA Mod. Hrg. at 18 ("massive amounts of analytic resources" used "to craft FISA applications"). There is no reason to think that this is any less so in situations where the Government collects communications of non-U.S. persons located abroad via Upstream instead of PRISM.

Nevertheless, the Government further addresses Upstream's value to national security, to the extent possible in unclassified terms, in the public portions of the supplemental Classified Declaration of Miriam P., submitted herewith ("Nov. 7 Class. Miriam P. Decl."). As the public portions of the declaration confirm, the justifications for authorizing Section 702 collection without requiring individualized warrants apply to Upstream as well as PRISM collection, and imposing a warrant requirement each time a selector must be targeted for Upstream collection would result in the loss of critical foreign intelligence information. *Id.* ¶¶ 32-33.[18]

Plaintiffs also try to distinguish cases holding that the Government's special need for foreign intelligence information justifies an exception to the warrant requirement, *see* Gov't Mem. at 35-36, on the basis that they concerned PRISM not Upstream collection. But they fail here too to explain why the method of collection matters to the reasoning of these cases. Pls.' Opp. at 19-21. Courts have held that collection of foreign intelligence does not require a warrant because of the importance of the national interest in foreign-intelligence gathering above and beyond normal law enforcement, and because of the need for flexibility and timeliness in the collection of foreign intelligence, given its particular nature and objectives. *See* Gov't Mem. at 36. The justifications for excepting foreign-intelligence collection from the warrant requirement apply equally whether the Government collects intelligence as communications transit the Internet backbone (Upstream), directly from Internet service providers (PRISM), or, for that matter, pursuant to traditional FISA orders . *See* Nov. 7 Class. Miriam P. Decl. ¶¶ 32-33.[19]

[18] The classified information in Ms. P.'s supplemental declaration is not relied on here, § III, but is submitted in support of the Government's alternative argument, *infra*, § IV, at 20-21, that if Plaintiffs' Fourth Amendment claim is not rejected on the basis of the public record, then a full and fair adjudication of the special needs issue would require disclosure of information protected by the state secrets privilege, mandating dismissal of Plaintiffs' claim on that basis.

[19] Plaintiffs' additional criticism of *Mohamud*'s determination that the targeting and minimization procedures contribute to the reasonableness of Section 702 surveillance as

Accordingly, the special needs doctrine applies to the alleged real-time electronic copying and scanning of online communications, and these alleged activities must be upheld as reasonable, particularly insofar as they involve communications that the Government does not retain. Even if alleged Stage 1 copying and Stage 3 scanning of unretained communications were deemed seizures and searches, they involve minimal intrusions on Fourth Amendment interests and are necessary to an effective means of gathering foreign intelligence important to the protection of national security. *See supra*, at 7-11; Gov't Mem. at 25-29; 31-34; 39-42.

Seeking to resist this conclusion, Plaintiffs assert that the "duration" of the "electronic scanning" says nothing about its "intrusiveness," because the communications' contents are "examine[d]" from "top to bottom," Pls.' Opp. at 22. But these characterizations disregard the critical fact—under the program as Plaintiffs contend it operates, no information about the communications at issue is ever made known to Government personnel. Neither the law nor common-sense notions of privacy support treating as constitutionally indistinguishable the "intrusion" caused in a millisecond by an automated scan of communications that reveals no information about them, and the intrusion that would be wrought by Government agents poring for hours over the same set of communications in search of targeted selectors. *See supra*, at 10-11; *Cassidy v. Cherthoff*, 471 F.3d 67, 79 (2d Cir. 2006) (noting brevity and unintrusiveness of search); *MacWade*, 460 F.3d at 273 (same).[20]

---

inconsistent with "the Supreme Court's admonition [in *Riley v. California*, 134 S. Ct. 2473, 2491 (2014)] that 'government agency protocols' are no substitute for a warrant," Pls.' Opp. at 20-21, is off the mark. The targeting and minimization procedures for Section 702 surveillance are required by the statute and approved by the FISC (*see* Gov't Mem. at 6 n.1), not merely protocols voluntarily developed by government agencies (which can still factor into a totality-of-the-circumstances reasonableness analysis). *See Riley*, 134 S. Ct. at 2491.

[20] Plaintiffs also dispute that the putative searches here are less intrusive than those upheld by other courts, Pls.' Opp. at 23 n.14; Gov't Mem. at 39, because those cases (they assert) involved PRISM, not Upstream, collection. Plaintiffs again miss (or ignore) the point. Those cases involved communications that had been retained by the Government; the instant motion does not. Plaintiffs also attempt to dismiss various statutory safeguards such as restrictions on targeting and the purposes for which communications may be acquired, reporting requirements to facilitate Congressional oversight as "non sequitur[s]" when it comes to the reasonableness of "search[ing] the contents" of the communications. Pls.' Opp. at 22-23. But, although Plaintiffs challenge only the alleged initial stages of Upstream collection, their reasonableness still must be assessed in light of the ultimate programmatic purposes for which they are undertaken, measures to assess whether those purposes are being achieved, and protections ensuring that these activities are not conducted for purposes or in a manner unauthorized by the statute. *See* 50 U.S.C. § 1881a; *Samson v. California*, 547 U.S. 843, 848 (2006).

Plaintiffs also argue, without citation, that the alleged copying and scanning of unretained communications is unreasonable because there are "other practicable alternatives" to Upstream that are less intrusive, such as PRISM collection and traditional FISA surveillance orders. Pls.' Opp. at 17. But the special needs doctrine requires only that the Government employ "a reasonably effective means"—and not "the least intrusive means,"—of addressing the special need. *Board of Educ. of Indep. Sch. Dist. of Pottawatomie Co. v. Earls*, 536 U.S. 832, 837 (2002). The choice among reasonable alternatives "remains with the governmental officials who have a unique understanding of, and a responsibility for, limited public resources," *Sitz*, 496 U.S. at 453-54; *see also Martinez-Fuerte*, 428 U.S. at 566. Plaintiffs' speculation that the Government can accomplish the same goals through PRISM collection and traditional FISA warrants is simply irrelevant. It is also incorrect.

The Government has already shown that Upstream collection is a reasonably effective means of meeting its special need to obtain foreign intelligence information, a need Plaintiffs concede is "weighty." Gov't Mem. at 40-42; Pls.' Opp. at 16. Plaintiffs contend, however, that the Government's reliance on legislators' assessment of the importance and effectiveness of Section 702 surveillance (including Upstream) when Congress reauthorized the statute—an assessment based on numerous hearings and years of briefings from Executive Branch officials, Gov't Mem. at 41—is "no substitute for 'empirical evidence of the effectiveness'" of Upstream collection specifically. Pls.' Opp. at 23. The FISC has found, however, that "NSA's upstream collection is *uniquely* capable of acquiring certain types of targeted communications containing valuable foreign intelligence information." *[Redacted]*, 2011 WL 10945618, at *10 (FISC Oct. 3, 2011) (emphasis added). What can also be stated publicly is that Upstream collection is capable of acquiring certain valuable foreign intelligence that cannot be collected under PRISM or other methods authorized by FISA, Nov. 7 Class. Miriam P. Decl., ¶¶ 8, 12-13, 16, "fills a critical gap in U.S. intelligence gathering," *id.* ¶ 17, allows the NSA to respond quickly and effectively to developing threats, *id.*, and contributes "significant and sometimes uniquely valuable foreign intelligence necessary to protect the Nation's security," *id.* This assessment corroborates judgments jointly reached by the political Branches in adopting and reauthorizing

Section 702, is entitled to the Court's deference, Gov't Mem. at 41-42, and is plainly sufficient to award judgment to the Government on Plaintiffs' Fourth Amendment claim.

IV. IN THE ALTERNATIVE, PLAINTIFFS' FOURTH AMENDMENT CLAIM MUST BE DISMISSED BECAUSE IT CANNOT BE LITIGATED WITHOUT NATIONAL-SECURITY INFORMATION PROTECTED BY THE STATE SECRETS PRIVILEGE.

As set forth in the Government's opening brief and the classified *ex parte* supplement thereto, even if the Court were to conclude that Plaintiffs have presented competent evidence that Upstream collection involves either seizures or searches of Plaintiffs' communications, and that the minimal intrusion on Plaintiffs' Fourth Amendment interests is not outweighed by Upstream's contributions to national security, then in the alternative judgment still must lie for the Government. That is so because operational details about Upstream that are necessary to a full and fair adjudication of Plaintiffs' standing, their claims of Fourth Amendment seizures and searches, and the Government's defenses thereto, are subject to the DNI's assertion of the state secrets privilege, and excluded from the case. Gov't Mem. at 21, 43-45.

The same is now also true regarding the special needs analysis. Although Plaintiffs question the sufficiency of the public evidence demonstrating the importance and effectiveness of Upstream, Pls.' Opp. at 23, the NSA also possesses classified information, set forth in the supplemental Miriam P. declaration, regarding the operational details of the Upstream program that supports the Government's position on these points as well. Because these details cannot be disclosed without risking exceptionally grave damage to national security, they fall within the category of operational details concerning the Section 702 program, described in prior NSA declarations, on which the DNI based his assertions of the state secrets privilege. Nov. 7 Class. Miriam P. Decl. ¶¶ 5, 34. Therefore, this information, too, must be "completely removed from the case." *Kasza v. Browner*, 133 F.3d 1159, 1166 (9th Cir. 1998). For this additional reason, the state secrets doctrine requires that Plaintiffs' Fourth Amendment claim be dismissed, even barring all other grounds on which judgment should be awarded to the Government.

Plaintiffs err when they argue that the state secrets privilege has no application here because their motion is based solely on public evidence. Pls.' Opp. at 32. Although judgment should be entered *for the Government* based on the publicly available evidence, if the Court

determined otherwise then in the alternative Plaintiffs' claim would still have to be dismissed because a full and fair adjudication of the claim and the Government's defenses thereto would require harmful disclosures of national-security information that is protected by the state secrets privilege and must be excluded from the case. Gov't Mem. at 43.

Beyond that point, Plaintiffs repeat arguments to which the Government has previously responded. Pls.' Opp. at 33-34. FISA section 106, 50 U.S.C. § 1806(f), does not preclude assertion of the state secrets privilege here, even under the Court's prior ruling regarding § 1806(f). Gov't Mem. at 45 n.17. The valid defense prong of the state secrets doctrine is not limited to Government contracting cases, Gov't Defs.' Reply in Support of 2d Mot. to Dismiss & for Summ. Judg. (ECF No. 119) at 6-7, and turns not on the actual validity of a defense but the unavailability of the evidence required to support it. *Id.* at 11 & n.17. Plaintiffs' assertion that the Government "has not proven up any 'demonstrably valid' defense" is entitled to no weight, because they are not privy to the classified operational details regarding the Upstream program that support the Government's additional defenses.

CONCLUSION

For the reasons stated above, the Government's cross-motion for partial summary judgment on Plaintiffs' Fourth Amendment claim should be granted.

Dated: November 7, 2014

Respectfully submitted

JOYCE R. BRANDA
Acting Assistant Attorney General

JOSEPH H. HUNT
Director, Federal Programs Branch

ANTHONY J. COPPOLINO
Deputy Branch Director

/s/ James J. Gilligan
JAMES J. GILLIGAN
Special Litigation Counsel

MARCIA BERMAN
Senior Trial Counsel

RODNEY PATTON
Trial Attorney

JULIA BERMAN
Trial Attorney

U.S. Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Avenue, N.W., Room 6102
Washington, D.C. 20001
Phone: (202) 514-3358
Fax: (202) 616-8470
E-mail: james.gilligan@usdoj.gov

Attorneys for the Government Defendants