

1 JOYCE R. BRANDA
Acting Assistant Attorney General

2

3 JOSEPH H. HUNT
Director, Federal Programs Branch

4 ANTHONY J. COPPOLINO
Deputy Branch Director

5

6 JAMES J. GILLIGAN
Special Litigation Counsel

7 MARCIA BERMAN
Senior Trial Counsel

8

9 RODNEY PATTON
Trial Attorney

10 JULIA BERMAN
Trial Attorney

11

12 U.S. Department of Justice, Civil Division
20 Massachusetts Avenue, NW, Rm. 6102
Washington, D.C. 20001
13 Phone: (202) 514-3358; Fax: (202) 616-8470
14 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’
OPPOSITION TO PLAINTIFFS’
MOTION FOR PARTIAL SUMMARY
JUDGMENT AND CROSS-MOTION
FOR PARTIAL SUMMARY
JUDGMENT ON PLAINTIFFS’
FOURTH AMENDMENT CLAIM**

Date: October 31 and November 3, 2014
Time: 9:00 a.m.
Courtroom 5, Second Floor
Hon. Jeffrey S. White

TABLE OF CONTENTS

	PAGE
INTRODUCTION	1
BACKGROUND	4
A. The Foreign Intelligence Surveillance Act and the FISA Amendments Act of 2008	4
B. Operation of the Section 702 Program and Upstream Collection.....	6
C. Plaintiff’s Motion for Partial Summary Judgment.....	7
ARGUMENT	11
I. PLAINTIFFS’ MOTION SHOULD BE DENIED AS PROCEDUARLLY IMPROPER.....	11
II. NEITHER THE KLEIN AND MARCUS DECLARATIONS NOR THE MEDIA REPORTS CITED BY PLAINTIFFS CONSTITUTE ADMISSIBLE EVIDENCE TO SUPPORT THEIR STANDING OR FOURTH AMENDMENT CLAIMS	13
A. The Klein Declaration Is Not Competent Evidence Because It Is Based on Hearsay and Speculation, Rather Than Personal Knowledge	14
B. The Marcus Declaration Is Not Competent Evidence Because It Offers Improper Opinion Testimony Based on the Inadmissible Klein Declaration	16
C. Even if the Klein and Marcus Declarations Were Not Based on Speculation and Hearsay, They Could Not Support Plaintiffs’ Current Standing or the Merits of Their Fourth Amendment Claim	18
D. The Unsubstantiated Media Reports on Which Plaintiffs Rely Constitute Inadmissible Hearsay, and Are Entitled to no Weight	19
III. PLAINTIFFS HAVE NOT ESTABLISHED THEIR STANDING. AND CANNOT DO SO WITHOUT RISK OF GRAVE DAMAGE TO NATIONAL SECURITY	20
A. Plaintiffs Have Not Carried Their Evidentiary Burden of Establishing their Standing	20

B. Even if Plaintiffs Had Presented Admissible Evidence to Support Their Standing, the State Secrets Doctrine Would Still Require Entry of Judgment for the Government on the Standing Issue21

IV. PLAINTIFFS SHOULD BE DENIED SUMMARY JUDGMENT, AND JUDGMENT SHOULD INSTREAD BE AWARDED TO THE GOVERNMENT, ON THE MERITS OF PLAINTIFFS’ FOURTH AMENDMENT CLAIM23

A. Plaintiffs’ Claim of a Seizure at “Stage 1” Fails as a Matter of Fact and Law23

1. Plaintiffs have presented no admissible evidence that Upstream collection under Section 702 in fact involves the “Stage 1” seizure they allege24

2. Even if proven, the alleged “Stage 1” splitting of the Internet communications stream would not constitute a Fourth Amendment seizure as a matter of law25

3. No authority cited by Plaintiffs supports their seizure claim.....29

B. Plaintiffs’ Claim That Alleged “Stage 3” Scanning Constitutes a Search of Communications Not Found To Contain Targeted Selectors Is Also Without Merit31

C. The “Stage 1” Seizure and “Stage 3” Search Alleged by Plaintiffs Fall Within the Fourth Amendment’s “Special Needs” Doctrine and Are Reasonable Under the Totality of the Circumstances.....34

1. The challenged surveillance activities do not require the issuance of a warrant upon probable cause because the Government has a “special need” to collect foreign-intelligence information34

2. The challenged “Stage 1” copying and “Stage 3” scanning of Plaintiffs’ unretained communications are reasonable because the interests of national security far outweigh the minimal intrusion on Plaintiffs’ Fourth Amendment interests.....38

D. Even if Plaintiffs Had Presented Evidence of a Seizure or Search, Not Justified Under the Special Needs Doctrine, Their Fourth Amendment Claim Still Could Not Be Litigated Without National-Security Information Protected by the State Secrets Privilege.....43

CONCLUSION.....45

TABLE OF AUTHORITIES

CASES	PAGE(S)
<i>Al-Haramain Islamic Found. v. Bush</i> , 507 F.3d 1190 (9th Cir. 2007)	44
<i>In re Application of the United States of America for a Search Warrant for Contents of Electronic mail [etc.]</i> , 645 F. Supp. 2d 1210 (D. Or. 2009)	29
<i>Arizona v. Hicks</i> , 480 U.S. 321 (1987).....	27, 29
<i>Berger v. New York</i> , 388 U.S. 41 (1967).....	36
<i>Board of Educ. of Indep. Sch. Dist. No. 92 of Pottawatomie Cnty. v. Earls</i> , 536 U.S. 822 (2002).....	40, 43
<i>Bras v. Cal. Pub. Utils. Comm'n</i> , 59 F.3d 869 (9th Cir. 1995)	13, 18
<i>Cassidy v. Cherthoff</i> , 471 F.3d 67 (2d Cir. 2006).....	37, 43
<i>Celotex Corp. v. Catrett</i> , 477 U.S. 317 (1986).....	13, 20, 21
<i>City of Indianapolis v. Edmond</i> , 531 U.S. 32 (2000).....	35
<i>Clapper v. Amnesty Int'l USA</i> , 133 S. Ct. 1138 (2013).....	<i>passim</i>
<i>Courtney v. Canyon Television & Appliance Rental, Inc.</i> , 899 F.2d 845 (9th Cir. 1990)	14
<i>DMC Closure Aversion Comm. v. Goia</i> , 2014 U.S. Dist. LEXIS 121644 (N.D. Cal. Aug. 29, 2014).....	19
<i>De Boer v. Pennington</i> , 206 F.3d 857 (9th Cir. 2000)	25
<i>In re Directives</i> , 551 F.3d 1004 (FISC Ct. Rev. 2008).....	<i>passim</i>

<i>Electronic Frontier Foundation v. Dep't of Justice</i> , 2014 WL 3945646 (N.D. Cal. Aug. 11, 2014)	22
<i>Feezor v. Patterson</i> , 896 F. Supp. 2d 895 (E.D. Cal. 2012)	13
<i>Ferguson v. City of Charleston</i> , 532 U.S. 67 (2001).....	35
<i>Florida v. Jardines</i> , 133 S. Ct. 1409 (2013).....	30, 31
<i>Griffin v. Wisconsin</i> , 483 U.S. 868 (1987).....	35
<i>Haig v. Agee</i> , 453 U.S. 280, 307 (1981).....	39
<i>Hepting v. AT&T</i> , 439 F. Supp. 2d 974 (N.D. Cal. 2006)	22, 30
<i>Holder v. Humanitarian Law Project</i> , 561 U.S. 1 (2010).....	39, 41, 42
<i>Illinois v. Caballes</i> , 543 U.S. 405 (2005).....	31, 33
<i>Jewel v. NSA</i> , 965 F. Supp. 2d 1090 (N.D. Cal. 2013)	<i>passim</i>
<i>Kasza v. Browner</i> , 133 F.3d 1159 (9th Cir. 1998)	<i>passim</i>
<i>Lujan v. Defenders of Wildlife</i> , 504 U.S. 555 (1992).....	20, 21
<i>MacWade v. Kelly</i> , 460 F.3d 260 (2d Cir. 2006).....	43
<i>Marcus v. Search Warrants of Property</i> , 367 U.S. 717 (1961).....	29
<i>Maryland v. King</i> , 133 S. Ct. 1958 (2013).....	38, 39, 40, 43

<i>Mohamed v. Jeppesen Dataplan, Inc.</i> , 614 F.3d 1070 (9th Cir. 2010)	44, 45
<i>National Treas. Employees Union v. Von Raab</i> , 489 U.S. 656 (1989).....	35
<i>New Jersey v. T.L.O.</i> , 469 U.S. 325 (1985).....	35
<i>In re Oracle Corp. Sec. Litig.</i> , 627 F.3d 376 (9th Cir. 2010)	13
<i>Ortega v. O'Connor</i> , 146 F.3d 1149 (9th Cir. 1998)	19
<i>Pennsylvania v. Mimms</i> , 434 U.S. 106 (1977).....	34
<i>Raglin v. UPS</i> , 1997 U.S. App. LEXIS 13941	14
<i>Riley v. California</i> , 134 S. Ct. 2473 (2014).....	29
<i>Samson v. Maryland</i> , 547 U.S. 843 (2006).....	39
<i>In re Sealed Case</i> , 310 F.3d 717 (FISA Ct. Rev. 2002).....	36, 37
<i>In re Search of Information Associated with [Redacted] at mac.com [etc.]</i> , 2014 WL 1377793 (D.D.C. Apr. 7, 2014).....	28
<i>Segura v. United States</i> , 468 U.S. 796 (1984).....	25, 30
<i>Smith v. Chase Mtg. Credit Corp.</i> , 653 F. Supp. 2d 1035 (E.D. Cal. 2009)	13
<i>Stanford v. Texas</i> , 379 U.S. 476 (1965).....	29
<i>Stewart v. Wachowski</i> , 574 F. Supp. 2d 1074 (C.D. Cal. 2005)	19

<i>Stonefire Grill, Inc. v. FGF Brands, Inc.</i> , 987 F. Supp. 2d 1023 (C.D. Cal. 2013)	14
<i>Szajer v. City of Los Angeles</i> , 632 F.3d 607 (9th Cir. 2010)	19
<i>Tenenbaum v. Simonini</i> , 372 F.3d 776 (6th Cir. 2004)	45
<i>In re Terrorist Bombings of U.S. Embassies in E. Africa</i> , 552 F.3d 157 (2d Cir. 2008).....	43
<i>Terry v. Ohio</i> , 392 U.S. 1 (1968)	35
<i>Texas v. Brown</i> , 460 U.S. 730 (1983).....	25
<i>United States v. Bin Laden</i> , 126 F. Supp. 2d 264 (S.D.N.Y. 2000)	25
<i>United States v. Brown</i> , 884 F.2d 1309 (9th Cir. 1989)	25
<i>United States v. Buck</i> , 548 F.2d 871 (9th Cir. 1977)	35
<i>United States v. Clutter</i> , 674 F.3d 980 (8th Cir. 2012)	25
<i>United States v. DeMoss</i> , 279 F.3d 632 (8th Cir. 2002)	27
<i>United States v. Duka</i> , 671 F.3d 329 (3d Cir. 2011).....	35, 36, 37
<i>United States v. Elmore</i> , 304 F.3d 557 (6th Cir. 2002)	25
<i>United States v. England</i> , 971 F.2d 419 (9th Cir. 1992)	25, 26
<i>United States v. Gant</i> , 112 F.3d 241-42 (6th Cir. 1997).....	27

<i>United States v. Gill</i> , 280 F.3d 923 (9th Cir. 2002)	26
<i>United States v. Gorshkov</i> , 2001 WL 1024026 (W.D. Wash. May 23, 2001).....	29
<i>United States v. Hall</i> , 978 F.2d 616 (10th Cir. 1992)	27, 28
<i>United States v. Harvey</i> , 961 F.2d 1361 (8th Cir. 1992)	27
<i>United States v. Hoang</i> , 486 F.3d 1156 (9th Cir. 2007)	26
<i>United States v. Jacobsen</i> , 466 U.S. 109 (1984).....	<i>passim</i>
<i>United States v. Jefferson</i> , 566 F.3d 928 (9th Cir. 2009)	25, 26
<i>United States v. Jones</i> , 132 S. Ct. 945 (2012).....	30, 31, 42
<i>United States v. Kow</i> , 58 F.3d 423 (9th Cir. 1995)	30
<i>United States v. LaFrance</i> , 879 F.2d 1 (1st Cir. 1989).....	26
<i>United States v. Martinez-Fuerte</i> , 428 U.S. 543 (1976).....	35
<i>United States v. Mohamud</i> , 2014 WL 2866749 (D. Or. June 24, 2014) 2011 WL 10945618 (F.I.S.C. Oct. 3, 2011).....	<i>passim</i>
<i>United States v. Place</i> , 462 U.S. 696 (1983).....	<i>passim</i>
<i>United States v. Reynolds</i> , 345 U.S. (1953)	44
<i>United States v. Saboonchi</i> , 990 F. Supp. 2d 536 (D. Md. 2014)	29

United States v. Schofield,
80 Fed. Appx. 798, 802-03 (3d Cir. 2003).....27

United States v. Tamura,
694 F.2d 591 (9th Cir. 1982)30

United States v. Truong Dinh Hung,
629 F.2d 908 (4th Cir. 1980) *passim*

United States v. U.S. Dist. Ct. (Keith),
407 U.S. 297 (1972).....35, 36

United States v. Va Lerie,
424 F.3d 694 (8th Cir. 2005)25

United States v. Verdugo-Urquidez,
494 U.S. 259 (1990).....40

United States v. Zacher,
465 F.3d 336 (8th Cir. 2006)26

Virginia v. Moore,
553 U.S. 164 (2008).....29

STATUTES

50 U.S.C. § 1801.....5, 6, 42

50 U.S.C. §§ 1803(a), 1804(a), 18054

50 U.S.C. § 1806(f)..... *passim*

50 U.S.C. § 1821.....6

50 U.S.C. § 1881..... *passim*

Protect America Act (“PAA”),
Pub. L. No. 110-55 (2007)5

FISA Amendments Act of 2008 (“FAA”),
Pub. L. No. 110-261 (2008)5

FISA Amendments Act Reauthorization Act of 2012,
Pub. L. No. 112-238, 126 Stat. 163142

FEDERAL RULES OF CIVIL PROCEDURE

Fed. R. Civ. P. 56(c)13, 14

FEDERAL RULES OF EVIDENCE

Fed. R. Evid. 60214

Fed. R. Evid. 70114
 Fed. R. Evid. 70217, 18
 Fed. R. Evid. 80114, 15
 Fed. R. Evid. 80214

LEGISLATIVE MATERIAL

154 Cong. Rec. S6097, S6122 (June 25, 2008)37
 S. Rep. No. 112-229, 112th Cong., 2d Sess. (Sept. 20, 2012)40
 H.R. Rep. 112-645 (I), 112th Cong., 2d Sess. (Aug. 2, 2012).....37, 39, 41
 H.R. Rep. 112-645(II), 112th Cong., 2d Sess. (Aug. 2, 2012)38, 41
 S. Rep. No. 95-604 (1977)4
 S. Rep. No. 95-701 (1978)5
 S. Rep. No. 110-209 (2007)5
 S. Rep. 112-174, 112th Cong., 2d Sess. (June 7, 2012).....38, 41, 46
 Intelligence Activities: Hrgs. Before the Sen. Select Comm. To Study Governmental
 Operations With Respect to Intelligence Activities, 94th Cong., Vol. V, 57-59
 (1975)30
Modernization of the Foreign Intelligence Surveillance Act: Hearing before
S. Select Comm. on Intel., 110th Cong., 1st Sess. (May 1, 2007).....5, 37

MISCELLANEOUS

Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program*
Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance
Act (July 2, 2014)7, 40, 41, 42
 The President's Review Group on Intelligence and Communications Technologies,
Liberty and Security in a Changing World at 145 (Dec. 12, 2013)42

INTRODUCTION

1
2 Plaintiffs filed this action six years ago alleging that the Government was then
3 conducting “an illegal and unconstitutional program of dragnet communications surveillance” in
4 which it acquires the phone calls and electronic communications, “both international and
5 domestic, of practically every American” Compl. for Const. & Statutory Violations (ECF
6 No. 1) ¶¶ 1, 9, 74-75. Plaintiffs’ motion for partial summary judgment also claims at the outset
7 to prove the existence of “an ongoing program of bulk, untargeted seizure [and search] of the
8 Internet communications of millions of innocent Americans.” Pls.’ Mot. for Partial Summ. Judg.
9 (ECF No. 261) (“Pls.’ Mot.”) at 1. In the end, however, Plaintiffs’ motion presents a
10 dramatically downsized case, one not supported by evidence. The “mass surveillance” depicted
11 in their papers, *id.*, is allegedly carried out under the National Security Agency’s (“NSA’s”)
12 acknowledged “Upstream collection” of communications pursuant to Section 702 of the Foreign
13 Intelligence Surveillance Act (“FISA”). As Plaintiffs purport to describe it, the collection
14 involves a process by which the stream of electronic communications traveling on the fiber-optic
15 network of a telecommunications-service provider is electronically copied, filtered to remove
16 wholly domestic communications, and then scanned for communications containing targeted
17 (*e.g.*, terrorist-associated) selectors, after which the copied communications *not* found to contain
18 such selectors—*the only communications that Plaintiffs place at issue in their motion*—are
19 destroyed within milliseconds of their creation, without ever having been seen by a human being.

20 Even this diminished version of the alleged “dragnet” surveillance is unsupported by
21 admissible evidence, and fails to describe either a seizure or search, much less an unreasonable
22 seizure or search, within the meaning of the Fourth Amendment. Plaintiffs’ motion must
23 therefore be denied, their claims dismissed, and judgment awarded instead to the Government,
24 for numerous reasons.

25 First, Plaintiffs’ motion should be denied as procedurally improper and unauthorized
26 under the procedures the Court established for the orderly resolution of the four threshold
27 questions on which the Court directed briefing. Consideration of Plaintiffs’ motion for summary
28 judgment on the merits of their Fourth Amendment claim should be deferred until the Court has

1 addressed both those threshold issues and the question of whether the allegations in Plaintiffs'
2 complaint encompass the Section 702 program at all.

3 Second, if the Court decides to entertain the question of summary judgment at this time,
4 then Plaintiffs' motion should be denied, their claims dismissed, and judgment awarded instead
5 to the Government, because Plaintiffs still have not established their standing to challenge
6 alleged ongoing collection of communications by the NSA. At the summary-judgment stage,
7 Plaintiffs must present sufficient admissible evidence to support each essential element of their
8 claims, including their standing, or judgment must be awarded against them. As Plaintiffs
9 observe, the Government has acknowledged that Upstream involves the collection of certain
10 communications as they transit the Internet backbone networks of telecommunications-service
11 providers, but the technical details of the collection process remain classified. The Klein and
12 Marcus declarations that form the evidentiary basis of Plaintiffs' claim that the NSA seizes and
13 searches the online communications of millions of Americans, including theirs, rest on hearsay
14 and speculation about activities that allegedly occurred in 2002 and 2003, and are inadmissible to
15 prove anything about the scope, methods, or even the existence of current NSA intelligence-
16 gathering activities, including whether Plaintiffs' communications are acquired. Moreover,
17 although the failings of those declarations are dispositive of the standing question without
18 implication of state secrets, the Government has also explained in briefing on the Court's four
19 threshold questions that any attempt to adjudicate Plaintiffs' standing on grounds requiring
20 consideration of information subject to the Government's assertion of the state-secrets privilege
21 in this case, even in *ex parte* proceedings under 50 U.S.C. § 1806(f), risks harmful disclosure of
22 privileged national-security information. Thus, Plaintiffs' claims must be dismissed.

23 Third, even if Plaintiffs had established their standing, the Government, not Plaintiffs,
24 would still be entitled to summary judgment, because Plaintiffs have not shown as a matter of
25 fact or law that Upstream collection involves the seizures or searches of online communications
26 that they allege. Even if the evidence in the Klein and Marcus declarations was admissible and
27 Plaintiffs' description of Upstream collection were accepted as true, Plaintiffs still would not
28 succeed in demonstrating that the Government conduct assailed in their motion constitutes a

1 Fourth Amendment seizure or search. It is critical to understand, as Plaintiffs themselves
2 explain, Pls.' Mot. at 8-9, that the "seizure" and "search" they complain of do not involve
3 communications that are actually ingested by and retained in Government databases for further
4 review and analysis by Government personnel. Rather, Plaintiffs challenge as a seizure and
5 search, respectively, the electronic copying and scanning of those online communications that
6 the Government does *not* retain because they are not found when scanned to contain targeted
7 selectors. In Plaintiffs' own telling, those unretained communications are copied, scanned, and
8 then destroyed all within a matter of milliseconds, and they are never seen by any human being.
9 The process Plaintiffs allege does not meaningfully interfere with Plaintiffs' possessory interests
10 in their online communications, or reveal any information about them to Government personnel.
11 Thus, no Fourth Amendment seizure or search occurs as a matter of law.

12 Fourth, even if Plaintiffs had demonstrated a seizure and search of their online
13 communications not retained by the Government, the Government must prevail under the Fourth
14 Amendment's "special needs" doctrine. Because Upstream collection under Section 702 serves
15 the Government's interest in collecting foreign-intelligence information for the protection of
16 national security, information that as a practical matter cannot effectively be acquired by
17 warrant, Upstream collection falls under the "special needs" exception to the warrant
18 requirement. And Upstream collection meets the Fourth Amendment's essential requirement of
19 reasonableness, because the critical importance of the intelligence-collection capabilities
20 authorized by Section 702, as recognized by all three branches of the Government, far outweighs
21 the vanishingly small degree (if any) to which Upstream collection under the constraints imposed
22 by Section 702 and the Foreign Intelligence Surveillance Court ("FISC") infringes on Plaintiffs'
23 possessory or privacy interests in online communications that the Government does not acquire.

24 Finally, even if the Court determined that Plaintiffs have standing, and had presented
25 competent evidence of an unreasonable seizure or search, the state-secrets doctrine would still
26 entitle the Government to judgment. As explained in the classified supplement and Classified
27 Declaration of Miriam P., NSA, submitted *in camera*, *ex parte*, herewith, the Government
28 possesses detailed operational information about Upstream collection that is necessary to

1 adjudicate Plaintiffs' Fourth Amendment claim and the Government's defenses thereto, but
2 which is subject to the assertion of the state-secrets privilege in this case by the Director of
3 National Intelligence ("DNI"), and cannot be disclosed without risking exceptionally grave
4 damage to national security. In the alternative, therefore, the state-secrets doctrine requires that
5 Plaintiffs' claims be dismissed and judgment entered for the Government.

6 Lacking evidence or a legal basis to support even their pared-down claim of the dragnet
7 surveillance they once alleged, Plaintiffs repeatedly draw attention to the personal information
8 that can be gleaned from an individual's online communications, and appeal both to the Fourth
9 Amendment's core values and its historic purposes. But the Court need not overlook the
10 importance of individual privacy interests or forsake the core values of the Fourth Amendment to
11 conclude that Plaintiffs have not shown a violation of their Fourth Amendment rights. Even as
12 Plaintiffs describe it, the Upstream process, undertaken to promote critical national-security
13 interests, does not meaningfully encroach upon Plaintiffs' privacy or the values the Fourth
14 Amendment is meant to protect. Plaintiffs' motion for summary judgment should be denied,
15 their claims dismissed, and the Government's motion granted.

16 BACKGROUND

17 **A. The Foreign Intelligence Surveillance Act and the FISA Amendments** 18 **Act of 2008**

19 Congress enacted FISA in 1978 to place certain types of foreign-intelligence surveillance
20 under judicial oversight by requiring the Government to obtain an order authorizing such
21 surveillance from a FISC judge, based on probable cause to believe, *inter alia*, that the target of
22 the intended surveillance was a foreign power or an agent of a foreign power. *See* 50 U.S.C.
23 §§ 1803(a), 1804(a), 1805. When Congress enacted FISA, it focused on foreign-intelligence
24 surveillance of persons *within the United States*, *see* S. Rep. No. 95-604, at 7 (1977) (statute's
25 purpose is "to regulate the use of electronic surveillance within the United States for foreign
26 intelligence purposes"), by limiting the definition of "electronic surveillance," to which FISA's
27 requirements are keyed, to domestically targeted foreign-intelligence-collection activities. 50
28 U.S.C. § 1801(f). Congress intentionally excluded from FISA the vast majority of Government

1 surveillance then conducted outside the United States, even if it targeted U.S. persons abroad, or
2 incidentally acquired communications to or from U.S. persons or persons located in the U.S.
3 while targeting other parties abroad. *See* S. Rep. No. 95-701, at 7, 34-35, 71 (1978).

4 In 2006, Congress began considering modernization of FISA because changes in
5 communications technology had rendered its definition of electronic surveillance obsolete. *See*
6 S. Rep. No. 110-209, at 2-5 (2007); *Modernization of the FISA: Hrg. Before the S. Select Comm.*
7 *on Intel.*, 110th Cong., 1st Sess., 19 (May 1, 2007) (“May 1, 2007 FISA Mod. Hrg.”) (testimony
8 that FISA’s definition of “electronic surveillance” was “tie[d] . . . to a snapshot of outdated
9 technology”). Whereas international communications were predominantly carried by radio or
10 satellite when FISA was enacted (and so excluded from its definition of electronic surveillance),
11 they were now predominantly carried by fiber-optic cable, and qualified as wire communications
12 potentially included within FISA’s coverage. *Id.* at 18-19; *see* 50 U.S.C. § 1801(f)(2), (3)
13 (defining electronic surveillance under FISA). Furthermore, intercepts of wire or other non-radio
14 communications conducted inside the United States were covered under FISA, while those
15 conducted outside the U.S. generally were not. May 1, 2007 FISA Mod. Hrg. at 19; 50 U.S.C.
16 § 1801(f)(2). This was a distinction that technological advances had also rendered outmoded,
17 when “a single communication can transit the world even if the two people communicating are
18 only located a few miles apart.” May 1, 2007 FISA Mod. Hrg. at 19. Due to these technological
19 changes, the Government had to expend significant resources to craft numerous individual FISA
20 applications for surveillance that was originally intended to be outside FISA’s scope. *Id.* at 18.

21 Congress addressed this problem initially through the Protect America Act (“PAA”), Pub.
22 L. No. 110-55 (2007), and ultimately through its successor statute, the FISA Amendments Act of
23 2008 (“FAA”), Pub. L. No. 110-261 (2008). The FAA provision at issue here, Section 702 of
24 FISA, 50 U.S.C. § 1881a, “supplements pre-existing FISA authority by creating a new
25 framework under which the Government may seek the FISC’s authorization of certain foreign
26 intelligence surveillance targeting . . . non-U.S. persons located abroad,” *Clapper v. Amnesty*
27 *Int’l USA*, 133 S. Ct. 1138, 1144 (2013), without regard to the location of the collection. Section
28 702 provides that, upon the FISC’s approval of a “certification” submitted by the Government,

1 the Attorney General and the DNI may jointly authorize, for up to one year, the “targeting of
 2 [non-U.S.] persons reasonably believed to be located outside the United States to acquire foreign
 3 intelligence information.” 50 U.S.C. § 1881a(a), (g).¹ The statute does not define this authority
 4 by reference to particular technology, other than to specify that acquisitions of communications
 5 under Section 702 must involve “the assistance of an electronic communication service
 6 provider.” *Id.* § 1881a(g)(2)(A)(vi). Under the express terms of Section 702, the Government
 7 may not intentionally target any person known at the time of acquisition to be in the United
 8 States or any U.S. person reasonably believed to be located abroad, or intentionally acquire any
 9 communication known at the time of acquisition to be wholly domestic. *Id.* § 1881a(b). The
 10 acquisition must also be “conducted in a manner consistent with the [F]ourth [A]mendment.” *Id.*

11 **B. Operation of the Section 702 Program and Upstream Collection**

12 As summarized herein, the Government has described the collection of communications
 13 under Section 702, in general terms, in a number of public reports. Upon FISC approval of a
 14 certification under Section 702, NSA analysts identify non-U.S. persons located outside the
 15 United States who are reasonably believed to possess or receive, or are likely to communicate,
 16 foreign-intelligence information designated in the certification. Such a person might be an
 17 individual who belongs to a foreign terrorist organization or facilitates its activities. NSA Civil
 18 Liberties and Privacy Office Report, NSA’s Implementation of FISA Section 702 at 4 (Apr. 16,
 19 2014) (“Civ. Lib. Report”) (Exh. A hereto). Once the NSA has designated such a person as a
 20 target, it then tries to identify a specific means by which the target communicates, such as an e-
 21 mail address or a telephone number; that identifier is referred to as a “selector.” Selectors may
 22 not be key words or the names of targeted individuals, but must be specific communications

23 _____
 24 ¹ Four requirements must be met for FISC approval of a Section 702 certification. First,
 25 the FISC must find that the Government’s “targeting procedures” are reasonably designed to
 26 ensure that acquisitions conducted under the authorization (a) are limited to targeting non-U.S.
 27 persons reasonably believed to be located outside the United States, and (b) will not intentionally
 28 acquire communications known at the time of acquisition to be purely domestic. *Id.*
 § 1881a(i)(2)(B). Second, the FISC must find that the Government’s minimization procedures
 meet FISA’s requirements. *Id.* §§ 1801(h), 1821(4), 1881a(i)(2)(C). Third, the Attorney
 General and the DNI must certify, *inter alia*, that a significant purpose of the acquisitions is to
 obtain foreign-intelligence information. *Id.* § 1881a(g)(2)(A)(v), (i)(2)(A). And fourth, the
 FISC must find that the Government’s targeting and minimization procedures are consistent, not
 only with FISA, but also with the requirements of the Fourth Amendment. *Id.* § 1881a(i)(3)(A).

1 accounts, addresses or identifiers. *Id.*; Intelligence Community’s Collection Programs under
2 Title VII of the FISA at 3 (“IC’s Coll. Programs”) (Exh. B hereto); Privacy & Civil Liberties
3 Oversight Bd. Report on the Surveillance Program Operated Pursuant to Section 702 of the FISA
4 at 32-33, 36 (“PCLOB Report”) (Exhibit C hereto). An electronic-communications-service
5 provider may then be compelled to provide the Government all information or assistance
6 necessary to acquire communications associated with the selector, a process referred to as
7 “tasking.” PCLOB Report at 32-33; Civ. Lib. Report at 4-5.

8 One method through which NSA receives information concerning tasked selectors is
9 known as “Upstream collection.” Upstream collection occurs as communications “transit the
10 Internet ‘backbone’ within the United States.” IC’s Coll. Programs at 3. *See also* PCLOB
11 Report at 35. Under Upstream collection, tasked selectors are sent to a U.S. electronic-
12 communications-service provider to acquire communications that are transiting the Internet
13 backbone. PCLOB Report at 36-37. Internet communications are first filtered to eliminate
14 potential domestic communications, and are then scanned to capture only communications
15 containing the tasked selector. *Id.* at 37. “Unless [communications] pass both these screens,
16 they are not ingested into government databases.” *Id.* (quoted in Pls.’ Mot. at 9). Further
17 operational details regarding the mechanics of Upstream collection remain classified. *See, e.g.,*
18 Classified Declaration of Miriam P., submitted *in camera, ex parte* herewith.

19 **C. Plaintiff’s Motion for Partial Summary Judgment**

20 Plaintiffs’ motion for partial summary judgment seeks a determination that the
21 Government Defendants, through Upstream collection under Section 702, are currently violating
22 the Fourth Amendment by seizing and searching Plaintiffs’ Internet communications. *See* Pls.’
23 Mot. at 1, 9, 21. Plaintiffs state that they are not, in this motion, challenging any past activities
24 that allegedly occurred under presidential authorization, or the legality of the Government’s
25 collection of telephone communications, telephony metadata, or Internet metadata. *See id.*

26 The moving Plaintiffs, Jewel, Knutzen, and Walton, claim at different times to have been
27 subscribers to AT&T’s WorldNet Internet service, and they now claim to be subscribers to other
28 AT&T Internet services. Jewel Decl. ¶¶ 2-3; Knutzen Decl. ¶¶ 2-3; Walton Decl. ¶¶ 2-3.

1 Although the Government has not revealed the operational details of Upstream collection and
2 those details remain classified, Plaintiffs base their claim that Upstream collection involves
3 unreasonable seizures and searches of their online communications on their own understanding
4 of Upstream collection as a four-stage process.² First, according to Plaintiffs, their Internet-
5 service provider, AT&T, “creates and delivers to the government” a copy of “the entire stream of
6 domestic and international [Internet] communications” carried by AT&T’s fiber optic cables,
7 presumably including copies of their communications along with those of millions of other
8 Americans. Pls.’ Mot. at 2, 4-6, 10. Plaintiffs claim these copies are made as the
9 communications flow through junctions (peering links) between AT&T’s network and other
10 providers’ networks on the Internet backbone. *Id.* at 4 & n.3. Plaintiffs assert that the copying is
11 accomplished using “splitters,” devices that split the light signals on AT&T’s fiber-optic cables
12 to make identical copies of the communications carried on the cables. *Id.* at 6. The splitters
13 allow a copy of the communications stream to be “diverted for further processing and searching
14 by the NSA,” while still allowing the original stream “to travel as it normally would to its
15 intended destination on the Internet.” *Id.* Plaintiffs refer to this process as “stage one” of the
16 alleged surveillance (“Stage 1”). *Id.* at 5-6.

17 Next Plaintiffs assert that, at “stage two” (“Stage 2”), the copied communications are
18 filtered for foreignness, that is, to remove purely domestic communications from the copied
19 stream. *Id.* at 6. According to Plaintiffs, the copied and filtered communications stream is
20 “searched” at “stage three” (“Stage 3”) for particular selectors, such as email addresses and
21 phone numbers, associated with individual targets. *Id.* at 6-9. The results are “deposited into
22 government databases for retention” at “stage four” (“Stage 4”). *Id.* at 8. ““Only those
23 communications . . . that contain a tasked selector”” are so retained. *Id.* at 9 n.14 (quoting
24 PCLOB Report at 111 n.476).

25 Plaintiffs’ evidentiary foundation for claimed Stages 1 and 2 rests on two declarations
26 filed by Plaintiffs in 2006 in *Hepting v. AT&T*, Case No. 06-CV-0676 (N.D. Cal.): the

27 ² To support their assertions regarding activities conducted at the first two stages,
28 Plaintiffs rely on the inadmissible assertions in the Klein and Marcus declarations. As to the
third and fourth stages, Plaintiffs rely largely, albeit not entirely, on facts stated about Upstream
collection in Government reports, discussed *supra* at 6-7. See Pls.’ Mot. at 6-8 & n.9, 11-14.

1 Declaration of Mark Klein (“Klein Decl.”), a former AT&T employee who retired from AT&T
2 in May 2004, Klein Decl. ¶¶ 2-6, and the Declaration of J. Scott Marcus (“Marcus Decl.”), a
3 purported communications technology expert, Marcus Decl. ¶ 7. Pls.’ Mot. at 6 nn. 5-8. Mr.
4 Klein claims that in 2003, AT&T constructed a new equipment room, known as the “SG3 Secure
5 Room,” at its Folsom Street telecommunications facility in San Francisco, California. According
6 to Mr. Klein, the room was secured with multiple keyed and combination locks, and the regular
7 AT&T technician workforce was not allowed to enter. Klein Decl. ¶¶ 11-12, 17-18. Earlier in
8 2002 an individual, who another AT&T employee supposedly informed Mr. Klein was an NSA
9 agent, interviewed an AT&T Field Support Specialist for a “special job” at Folsom Street; the
10 specialist installed equipment in the SG3 Secure Room in January 2003. *Id.* ¶¶ 10, 14. In the
11 fall of 2003 another supposed NSA agent interviewed a second AT&T Field Support Specialist
12 who took over the “special job” at Folsom Street in January 2004. *Id.* ¶ 16.

13 At this time, AT&T provided Internet services to customers through its WorldNet
14 Internet service. *Id.* ¶ 19. Mr. Klein avers that the WorldNet Internet room at Folsom Street
15 contained telecommunications equipment used to direct e-mails, web-browsing requests, and
16 other Internet-based communications sent to and from customers of AT&T’s WorldNet Internet
17 service. *Id.* ¶¶ 15, 19. He asserts that in February 2003, a “splitter cabinet” was installed in the
18 WorldNet Internet Room at Folsom Street to duplicate the signals of certain (but not all) of the
19 fiber-optic circuits carrying WorldNet Internet services, and divert the duplicate signals to the
20 SG3 Secure Room, while allowing the original signals to continue as they previously had. The
21 split circuits allegedly were “peering links” that connected the WorldNet Internet network to the
22 networks of fourteen non-AT&T telecommunications companies and two Internet exchange
23 points. He states that the splitters transferred to the SG3 Secure Room the contents of all the
24 electronic voice and data communications going across those links. *Id.* ¶¶ 24-34; Marcus Decl.
25 ¶ 62. Mr. Marcus, based on his knowledge of “peering traffic patterns” in the industry, infers
26 that the copied communications constituted all or substantially all of AT&T’s off-net IP-based
27 traffic in the San Francisco Bay Area. Marcus Decl. ¶¶ 56, 61, 71-72, 104-08.

1 According to Mr. Klein, an AT&T business document attached to his declaration
2 indicates that the equipment installed in the SG3 Secure Room included a Narus STA 6400
3 Semantic Traffic Analyzer and a Narus Logic Server. Klein Decl. ¶ 35; *see also* Marcus Decl.
4 ¶¶ 44, 75. Mr. Marcus opines that the Narus system was a “key component” of the SG3
5 equipment configuration shown on the AT&T document, “designed” to analyze large volumes of
6 data in “real time,” at “true carrier” speeds, and was “well suited” to high-speed winnowing
7 down of large volumes of data to identify communications of interest for surveillance purposes.
8 *Id.* ¶¶ 44, 74, 75, 79-81, 83-85. He also considers it “highly likely” that the SG3 Secure Room
9 was connected to a second fiber-optic network other than AT&T’s, on which signals could be
10 sent out of or into the SG3 Secure Room, although he acknowledges that the documentation
11 provided by Mr. Klein “do[es] not . . . indicate [by] what entities.” *Id.* ¶¶ 76-77, 87.

12 Mr. Marcus also finds it “credible” that the SG3 Secure Room was intended for purposes
13 of surveillance on a substantial scale. *Id.* ¶ 6. He opines that the infrastructure constructed at
14 Folsom Street provided AT&T the “capacity” to assist the Government in carrying out
15 warrantless content surveillance of both the domestic and international IP-based communications
16 of people in the United States, with the early stages being “computer-controlled collection and
17 analysis of communications,” and the last stage being “actual human scrutiny.” *Id.* ¶¶ 3, 38-39;
18 *see also id.* ¶¶ 88, 90. The components allegedly chosen “[were] exceptionally well suited” to
19 massive, covert surveillance of IP-based data: massive data capture with high-speed scanning at
20 the capture point to identify data of interest, and shipment of those data to a collection point (or
21 points) for more detailed analysis. Mr. Marcus acknowledges that the alleged configuration
22 could have been used solely for commercial applications or routine intercepts, but in his view
23 was vastly in excess of that needed for applications other than surveillance. The most plausible
24 inference, he opines, is that it “was a covert network . . . used to ship data of interest to [] central
25 locations for still more intensive analysis.” *Id.* ¶¶ 40-43, 45, 47, 49, 88, 90, 129, 136.

26 Mr. Marcus finally opines that it is unlikely that AT&T would have made the necessary
27 financial investments to create the SG3 infrastructure given what he characterizes as its troubled
28 financial condition in 2003. The United States Government, he surmises, is “the most obvious

1 funding source,” supporting the “plausibility” of a government role in the SG3 configurations.
 2 *Id.* ¶¶ 46, 137, 146, 147. He also finds it “plausible” that other splitter cabinets like the one
 3 installed at Folsom Street were installed at AT&T facilities in Seattle, San José, Los Angeles,
 4 and San Diego, and is consistent with similar deployments at 15-20 AT&T sites. He found it
 5 “highly probable” that all or substantially all of AT&T’s traffic from other Internet Service
 6 Providers was diverted, including a substantial fraction, probably more than one half, of all
 7 AT&T domestic traffic, approximately ten percent of all domestic Internet communications in
 8 the United States. Klein Decl. ¶ 36; Marcus Decl. ¶¶ 113, 114, 118, 120, 124-126.

9 On the basis of these assertions regarding the capabilities of equipment allegedly located
 10 in a secure room at AT&T’s Folsom Street facility in 2003, but without evidence of their actual
 11 use or purpose (even then), Plaintiffs contend that the Government is *today* violating their Fourth
 12 Amendment rights in two ways. First, they maintain that the Government *seizes* their online
 13 communications at Stage 1 of the Upstream process when, as they describe it, AT&T “creates
 14 and delivers to the government” a copy of “the entire stream of domestic and international
 15 [Internet-based] communications” carried on its fiber-optic network. Pls.’ Mot. at 2, 6, 16-19.
 16 Second, Plaintiffs argue that after the copied communications stream is filtered, at alleged
 17 Stage 2 (the lawfulness of which they do not contest), to remove purely domestic
 18 communications, the remaining communications are *searched*, at Stage 3, to identify the
 19 communications, containing targeted selectors, that will be retained in Government databases for
 20 foreign-intelligence purposes. *Id.* at 6-9, 19-21. Plaintiffs state, without qualification, that “[t]he
 21 communications the [G]overnment retains at stage four are not at issue here,” and that their
 22 motion challenges only the claimed Stage 1 “seizure of the stream of Internet communications”
 23 and Stage 3 “searching . . . of the contents of those communications for selectors.” *Id.* at 9.

ARGUMENT

I. PLAINTIFFS’ MOTION SHOULD BE DENIED AS PROCEDURALLY IMPROPER.

24
 25
 26 Plaintiffs’ motion for summary judgment *on the merits* of their Fourth Amendment claim,
 27 as it relates to alleged ongoing seizures and searches of their Internet communications, should be
 28

1 denied as procedurally improper. Plaintiffs' motion is premature in light of the threshold legal
2 issues currently pending before the Court, and is unauthorized under the procedures the Court
3 established for the orderly resolution of those issues.

4 On July 23, 2013, the Court issued a decision on the parties' prior motions to dismiss or
5 for summary judgment, at the conclusion of which it ordered further briefing on issues
6 pertaining, *inter alia*, to Plaintiffs' standing. *Jewel v. NSA*, 965 F. Supp. 2d 1090, 1112-13 (N.D.
7 Cal. 2013). The Court held a case management conference on September 27, 2013 to discuss
8 and set a schedule for this further briefing, which the Court noted was on "important threshold
9 legal issues." Tr. of Proceedings dated September 27, 2013 ("Tr.") at 5. The Court required
10 additional briefing on, *inter alia*, whether Plaintiffs can establish their standing without
11 impermissible damage to national security, assuming procedures under 50 U.S.C. § 1806(f) may
12 be used here ("question three"). *Id.* at 6-7.

13 During the case management conference, counsel for Plaintiffs asked the Court whether
14 Plaintiffs could move for partial summary judgment on "one part of one claim where we think
15 we can prove our standing with public evidence," that is, "[their] Fourth Amendment claim" as it
16 relates to "current ongoing internet interceptions." Plaintiffs sought leave to address this issue
17 as part of their briefing on question three, whether they can establish their standing without
18 risking damage to national security. *Id.* at 19-20. The Court answered that such a motion was
19 permissible "[a]s it relates to standing." *Id.* at 20. As the transcript makes clear, the Court
20 authorized briefing on the limited issue of whether Plaintiffs could establish their standing to
21 bring a Fourth Amendment claim related to allegedly ongoing Internet interceptions, not full-
22 scale summary judgment briefing on the merits of such a claim. Yet that is what Plaintiffs have
23 filed. Plaintiffs' motion seeks to litigate the merits of one of their claims before the Court
24 resolves the threshold legal issues it identified, in disregard of the Court's clearly stated
25 instructions as to how the case should proceed.

26 In addition, the hotly disputed issue of whether Plaintiffs' complaint even includes the
27 claim on which they purport to move for summary judgment is currently before the Court for
28 decision. The parties have extensively briefed, in the context of their preservation dispute,

1 whether Plaintiffs' complaint—which alleges unlawful surveillance without any statutory or
 2 judicial authorization—even purports to challenge the legality of intelligence programs such as
 3 Upstream collection that are authorized by the FISC pursuant to Section 702 of the FISA. *See*
 4 ECF Nos. 229, 233, 235, 243, 253. As the Government has demonstrated at length, it does not.
 5 For this reason Plaintiffs are not permitted now to seek summary judgment on this unpled claim.
 6 It is “axiomatic” that claims not pled in a complaint “cannot be considered by a court at the
 7 summary judgment stage.” *Feezor v. Patterson*, 896 F. Supp. 2d 895, 903 (E.D. Cal. 2012); *see*
 8 *also Smith v. Chase Mtg. Credit Corp.*, 653 F. Supp. 2d 1035, 1041 n.6 (E.D. Cal. 2009). At the
 9 very least, Plaintiffs' motion for summary judgment should be held in abeyance pending the
 10 Court's decision on this and the other threshold issues now pending.³

11 **II. NEITHER THE KLEIN AND MARCUS DECLARATIONS NOR THE MEDIA**
 12 **REPORTS CITED BY PLAINTIFFS CONSTITUTE ADMISSIBLE EVIDENCE**
 13 **TO SUPPORT THEIR STANDING OR FOURTH AMENDMENT CLAIMS.**

14 “One of the principal purposes of the summary judgment rule is to isolate and dispose of
 15 factually unsupported claims.” *Celotex Corp. v. Catrett*, 477 U.S. 317, 323–24 (1986). Plaintiffs
 16 must support each element of their Fourth Amendment claim, including standing, “with the
 17 manner and degree of evidence required at the successive stages of the litigation.” *Bras v. Cal.*
 18 *Pub. Utils. Comm'n*, 59 F.3d 869, 872 (9th Cir. 1995) (quoting *Lujan v. Defenders of Wildlife*,
 19 504 U.S. 555, 561 (1992)). Plaintiffs must adduce admissible evidence establishing both their
 20 standing and the merits of their claim. *See* Fed. R. Civ. P. 56(c); *see also In re Oracle Corp. Sec.*
 21 *Litig.*, 627 F.3d 376, 385 (9th Cir. 2010) (“A district court's ruling on a motion for summary
 22 judgment may only be based on admissible evidence.”). If Plaintiffs “fail[] to make a showing
 23 sufficient to establish the existence of an element essential to [their] case, and on which [they]
 24 will bear the burden of proof at trial,” “Rule 56(c) mandates the entry of summary judgment”
 25 against them. *Celotex Corp.*, 477 U.S. at 322.

26 As the factual foundation for both their standing and the merits of their claims, Plaintiffs
 27 rely largely on Klein and Marcus Declarations. These declarations are the principal support for
 28 Plaintiffs' assertion that all Americans' communications—or at least all AT&T customers'

³ If the Court nonetheless decides to entertain Plaintiffs' motion, it should, in the interests of fairness and efficiency, consider the Government's cross-motion at the same time.

1 communications—are currently subject to “dragnet” seizure and search. *See* Pls.’ Mot. at 6.
2 According to Plaintiffs, “[t]he Klein and Marcus evidence . . . demonstrates the NSA’s bulk
3 seizure of the content of [P]laintiffs’ AT&T Internet communications from the Internet
4 backbone.” *Id.* at 10. Neither declaration provides any competent support for that claim.

5 **A. The Klein Declaration Is Not Competent Evidence Because It Is Based**
6 **on Hearsay and Speculation, Rather Than Personal Knowledge.**

7 Rule 56(c) requires that declarations submitted in support of a summary judgment motion
8 “be made on personal knowledge, set out facts that would be admissible in evidence, and show
9 that the . . . declarant is competent to testify on the matters stated.” Fed. R. Civ. P 56(c)(4).
10 Thus, *inter alia*, materials must be based on the declarant’s personal knowledge, *see* Fed. R.
11 Evid. 602, rather than hearsay, *see* Fed. R. Evid. 801, 802, or speculation, *see* Fed. R. Evid. 701.
12 *See also Stonefire Grill, Inc. v. FGF Brands, Inc.*, 987 F. Supp. 2d 1023, 1037 (C.D. Cal. 2013)
13 (on a motion for summary judgment, “the Court may not consider inadmissible hearsay evidence
14 which could not be presented in an admissible form at trial.”); *Raglin v. UPS*, 1997 U.S. App.
15 LEXIS 13941, at *10 (“[I]nadmissible hearsay will not be considered a ‘fact’ for the purposes of
16 summary judgment.”) (citing *Courtney v. Canyon Television & Appliance Rental, Inc.*, 899 F.2d
17 845, 851 (9th Cir. 1990)). The Klein Declaration fulfills none of these requirements.

18 Mark Klein, a technician employed by AT&T until 2004, executed his declaration in
19 2006. *See* Klein Decl. ¶¶ 2, 4. Plaintiffs rely on the Klein Declaration (and attached documents)
20 for a description of the “SG3 Secure Room” at AT&T’s Folsom Street facility, where Plaintiffs
21 claim the Government intercepted and copied AT&T customers’ Internet-based communications.
22 *See* Pls.’ Mot. at 6 nn.4–8. Mr. Klein purports to describe the installation and operation of the
23 equipment inside that room, and to establish the Government’s involvement in both. *See* Klein
24 Decl. ¶¶ 10–35. His declaration is the sole asserted factual basis for Plaintiffs’ claims in this
25 regard; as discussed in § II.B, *infra*, Mr. Marcus, Plaintiffs’ other declarant, does not purport to
26 have independent knowledge of the Folsom Street facility and instead draws the assumptions
27 underlying his discussion from Mr. Klein. But Mr. Klein admits he had no personal knowledge
28 of that room’s contents, or the operation of whatever equipment was installed there. According

1 to Mr. Klein, he did not install or operate the equipment in the SG3 Secure Room. *See id.* In
2 fact, he “was not allowed in the SG3 Secure Room” at all. *Id.* ¶ 17. He received neither a key,
3 nor the combination that he states was required for entry. *Id.* Mr. Klein admits he was in that
4 room only once, for “a couple of minutes” while another technician “showed [him] some poorly
5 installed cable.” *Id.* Thus, although Plaintiffs rely on Mr. Klein to establish the content and
6 purpose of the SG3 Secure Room, he is not qualified to offer testimony on either.

7 Mr. Klein claims that the SG3 Secure Room is the room into which a “splitter cabinet”
8 diverted signals of certain fiber-optic circuits carrying AT&T customers’ internet
9 communication; he claims a copy went to the SG3 Secure Room, and the original signal
10 continued on its path. *See id.* ¶¶ 24–34. But Mr. Klein can only speculate about what data were
11 actually processed in the SG3 Secure Room, how, and for what purpose, since he was never
12 involved in its operation. Indeed, having spent only a couple of minutes there, Mr. Klein cannot
13 describe what equipment was in that room, much less explain what function it performed.
14 Although Mr. Klein submits the document entitled “Study Group 3, LGX/Splitter Wiring, San
15 Francisco” and claims it “list[s] the equipment installed in the SG3 Secure Room,” *see id.* ¶ 35,
16 this statement is entitled to no weight since Mr. Klein has no means of knowing that. *See id.*
17 ¶ 17. Thus, while Mr. Klein notes that the list included “a Narus STA 6400 . . . ‘Semantic
18 Traffic Analyzer,’” *id.* ¶ 35, which Mr. Marcus claims was designed to analyze large volumes of
19 data and was “well suited” to sort large volumes of data quickly to identify communications of
20 interest for surveillance purposes, Mr. Klein does not claim the Narus STA 6400 was ever
21 *actually* delivered to or installed in the SG3 Secure Room. *See Klein Decl.* ¶ 35. As with all of
22 Mr. Klein’s statements regarding the content or function of the SG3 Secure Room, any testimony
23 about the equipment installed there should be disregarded as speculation or hearsay.

24 So, too, with Mr. Klein’s allegations about Government involvement at the Folsom Street
25 facility: his declaration reflects that he had no personal experience of alleged NSA activity there.
26 Instead, his claims about Government involvement are all based on hearsay, *see Fed. R. Evid.*
27 801(c), 802. Although Mr. Klein asserts that “NSA cleared and approved” a particular person
28 (“FSS #2”) for a “special job,” and that this person installed equipment in the SG3 Secure Room,

1 *see id.* ¶¶ 10, 14, he does not claim to have been present when that alleged clearance was issued,
 2 or to have been involved in that work. Instead, an unnamed AT&T employee allegedly told him
 3 “to expect a visit from [an] . . . NSA agent,” and he received an e-mail from management that
 4 “explicitly mentioned the NSA.” *Id.* ¶ 10. Such out-of-court statements, offered for the truth of
 5 the matters discussed therein, are inadmissible. So too with Mr. Klein’s claim that FSS #1 told
 6 [Mr. Klein] “the NSA agent” was to interview another unnamed individual (“FSS #2”) “for a
 7 special job,” and FSS #1’s claim that “another NSA agent would again visit” in fall 2003 to
 8 speak with FSS #3 about “tak[ing] over” FSS #2’s “special job.” *Id.* ¶ 16.⁴

9 Mr. Klein’s claim regarding splitter cabinets in other AT&T locations is no different. He
 10 asserts that, while working with “another AT&T technician, [he] learned . . . ‘splitter cabinets’
 11 were being installed in other cities, including Seattle, San Jose, Los Angeles and San Diego.” *Id.*
 12 ¶ 36. But Mr. Klein does not purport to have ever installed, serviced, or even *seen* those alleged
 13 splitter cabinets, or to have any personal knowledge of their purpose. Such hearsay evidence is
 14 entitled to no weight on a summary judgment motion.

15 In sum, the Klein Declaration rests on hearsay and speculation. Such testimony is
 16 inadmissible, and is not probative even of AT&T’s activities in the SG3 Secure Room, much less
 17 of any alleged nationwide Government intelligence-gathering programs.

18 **B. The Marcus Declaration Is Not Competent Evidence Because It Offers**
 19 **Improper Opinion Testimony Based on the Inadmissible Klein Declaration.**

20 Likewise, the Court should give no weight to the Marcus Declaration, which Plaintiffs
 21 offer as “an expert opinion on the implications of [the Klein Declaration its exhibits].” Marcus
 22 Decl. ¶ 1. The same provision of Rule 56(c) discussed above, applies to the Marcus Declaration;
 23 evidence relied upon on summary judgment must be admissible. *See supra* at 13. Opinion
 24 testimony from a witness proffered as an expert is admissible only if “[the] witness . . . is
 25 qualified as an expert by knowledge, skill, experience, training, or education;” “the testimony is
 26 based on sufficient facts or data;” “the testimony is the product of reliable principles and

27 ⁴ Mr. Klein asserts that NSA agents conducted the interviews discussed above, but fails to
 28 explain the basis for those statements. *See id.* ¶¶ 10, 16. Barring Mr. Klein’s presence at the
 alleged interviews, to which he does not attest, the statements could only be based on hearsay.
 Likewise, his statement that “[t]o [his] knowledge, only employees cleared by the NSA were
 permitted to enter the SG3 Secure Room,” has no apparent basis other than hearsay. *See id.* ¶ 17.

1 methods;” and the proffered expert “has reliably applied the principles and methods to the facts
2 of the case.” Fed. R. Evid. 702. The Marcus Declaration satisfies none of these requirements.

3 The Marcus Declaration was executed in 2006 by J. Scott Marcus, a consultant who had
4 held various “positions involving computers, data communications, economics, and public
5 policy,” Marcus Decl. ¶¶ 7, 27. He also claimed he had “some experience with AT&T’s
6 network” in that, “[w]hen AT&T initially entered the Internet business in 1995,” AT&T
7 contracted with his firm to provide services to AT&T customers. *Id.* ¶ 13. Mr. Marcus did not
8 claim to have been an AT&T employee, or to have any personal knowledge of the alleged “SG3
9 Secure Room.” *See id.* Nonetheless, based on the Klein Declaration and its exhibits, Mr.
10 Marcus purports to summarize “the architecture of the SG3 Configuration and its data
11 connectivity,” *id.* ¶ 64, opines on “the activities likely to be occurring” in the SG3 Secure Room,
12 *id.* ¶ 78, and opines that the Government paid for it. *Id.* ¶ 46.

13 Mr. Marcus’s testimony regarding the SG3 Secure Room and other AT&T facilities fails
14 to satisfy Rule 702’s requirement that a putative expert’s testimony must be “based on sufficient
15 facts or data.” Fed. R. Evid. 702(b). Mr. Marcus has no personal knowledge of these facilities,
16 and relies on the Klein Declaration regarding AT&T’s operations. But, as discussed *supra*, at
17 14-15, that declaration is itself based on hearsay and speculation, and cannot supply the “facts”
18 that Rule 702 requires. For this reason, Mr. Marcus’s conclusions regarding the capabilities of
19 the equipment described by Mr. Klein, or the likely uses of the SG3 Secure Room, are all
20 speculation; there is no evidence in the record from a witness with personal knowledge of the
21 actual contents of the SG3 Secure Room or the uses to which the equipment was put.

22 For example, the Court cannot rely on Mr. Marcus’s discussion about the capabilities of
23 the Narus system as a “key component” of the SG3 Secure Room, including his conclusion that
24 it was “well suited” to high-speed winnowing down of large volumes of data to identify
25 communications for surveillance purposes, *see* Marcus Decl. ¶¶ 44, 74, 75, 79–81, 83–85, since
26 there is no competent evidence that such a system was actually installed or used there in the first
27 place, *see supra* at 15. Likewise, his testimony about the “plausibility” of Mr. Klein’s claims
28 regarding splitters to be installed in other AT&T facilities only adds speculation to the hearsay

1 testimony of Mr. Klein, *see supra* 14-15. But on summary judgment, parties must establish the
 2 facts necessary to their claims “with the manner and degree of evidence required at the
 3 successive stages of the litigation.” *Bras*, 59 F.3d at 872. The proffered evidence that Mr.
 4 Klein’s inadmissible allegations are “plausible,” and so could be true, falls far short of the mark.

5 Mr. Marcus’s claim that the Government funded the SG3 Secure Room is also
 6 inadmissible, not only because it is based on Mr. Klein’s inadmissible descriptions of that
 7 facility, but also because Mr. Marcus is not qualified to render such an opinion, and there is no
 8 evidence that he applied reliable methods to reach his conclusions. *See* Rule 702(c), (d). Mr.
 9 Marcus acknowledges that he “do[es] not consider [himself] an economist,” Marcus Decl. ¶ 29,
 10 and he has had no economics or corporate-finance training, *see id.*, Exh. A. Mr. Marcus offers
 11 no explanation of the methods he used or the facts he relied on to assess AT&T’s financial
 12 condition during the relevant timeframe, *see id.* ¶¶ 128–147, much less of their reliability, or the
 13 reliability of their application in this case. *See id.* Under Rule 702, Mr. Marcus’s assessments of
 14 how AT&T would have behaved based on its financial condition, and what projects it would
 15 have funded in 2003, are not admissible evidence and therefore are not competent to support
 16 Plaintiffs’ standing or Fourth Amendment claim on summary judgment.⁵

17 **C. Even if the Klein and Marcus Declarations Were Not Based on Speculation**
 18 **and Hearsay, They Could Not Support Plaintiffs’ Current Standing or the**
 19 **Merits of Their Fourth Amendment Claim.**

20 Plaintiffs emphasize that their Fourth Amendment claim addresses *ongoing*,
 21 nationwide intelligence-gathering activities. *See* Pls.’ Mot. at 1. But, even if their content were
 22 admissible, the Klein and Marcus Declarations would be probative only of events that occurred
 23 between 2002 and 2003, at least five years before Section 702 was even enacted. *See* Klein
 24 Decl. ¶¶ 10–18. Both declarations were executed in 2006, and are based on Mr. Klein’s account
 25 of events that allegedly occurred ten to twelve years ago. *See id.* Because over a decade has

26 ⁵ Additionally, even if it were based on admissible evidence and the proffered expert
 27 testimony were proper under Rule 702, the Marcus Declaration is contrary to the rule that, “[i]n
 28 considering a motion for summary judgment, the court . . . is required to draw all inferences in a
 light most favorable to the non-moving party.” *Jewel v. NSA*, 965 F. Supp. 2d 1090, 1099 (N.D.
 Cal. 2013) (citation omitted). Mr. Marcus repeatedly urges this Court to do just the opposite—to
 accept inferences uniformly favorable to the Plaintiffs’ case. *See, e.g.*, Marcus Decl. ¶¶ 40, 42
 (acknowledging, but asking the Court to ignore, that the SG3 Configurations could be used for
 commercial applications or routine intercepts).

1 elapsed since these alleged events, this information is too stale to be admissible. *Ortega v.*
2 *O'Connor*, 146 F.3d 1149, 1162 (9th Cir. 1998) (rejecting ten-year-old complaint of improper
3 conduct as basis for search for evidence of harassment); *see also Szajer v. City of Los Angeles*,
4 632 F.3d 607, 612 (9th Cir. 2010) (finding evidence five to fifteen years old “patently stale”).

5 Similarly, while Plaintiffs ask the Court to conclude, on the strength of these declarations,
6 that the Government’s activities at “stage one” “giv[e] it access to the entire stream of domestic
7 and international communications . . . carried on the fiber-optic cables of [the nation’s leading
8 telecommunications carriers, including AT&T],” Pls.’ Mot. at 6, the information in the
9 declarations does not extend nearly so far. Even if accepted as probative of events at the Folsom
10 Street facility, these declarations can establish only the events at that location. For example, that
11 Mr. Klein may have heard, from an unnamed source, of plans to install splitter cabinets in four
12 additional AT&T locations for some unknown purpose, *see* Klein Decl. ¶ 36, cannot establish
13 that the Internet communications of all AT&T customers, much less all Americans, are copied as
14 part of the alleged Stage 1 process; nothing in the Klein and Marcus Declarations supports such
15 an inferential leap.

16 Both as to the timeframe and the scope of the alleged intelligence-gathering activities, the
17 Klein and Marcus Declarations fall far short of the factual showing required of Plaintiffs at the
18 summary judgment stage of a legal proceeding.

19
20 **D. The Unsubstantiated Media Reports on Which Plaintiffs Rely Constitute
Inadmissible Hearsay, and Are Entitled to no Weight.**

21 While Plaintiffs largely rely on the Klein and Marcus Declarations, they also cite a
22 number of unsubstantiated media reports in support of their Fourth Amendment claim. *See, e.g.,*
23 Pls.’ Mot. 3–4 (discussing *Washington Post* articles); *id.* at 10 n.15 (citing articles from the *Wall*
24 *Street Journal* and the *New York Times*). Such media reports are hearsay and inadmissible on a
25 motion for summary judgment. *See, e.g., DMC Closure Aversion Comm. v. Goia*, 2014 U.S.
26 Dist. LEXIS 121644, at *28, n.12 (N.D. Cal. Aug. 29, 2014); *Stewart v. Wachowski*, 574 F.
27 Supp. 2d 1074, 1090 (C.D. Cal. 2005). Accordingly, the Court here should give no weight to the
28 media reports that Plaintiffs cite.

1 In sum, while Plaintiffs claim the Government currently conducts “indiscriminate,
2 suspicionless seizures” of their Internet communications, Pls.’ Mot. at 25, they have come
3 forward with no admissible evidence to support that claim. Where the party ultimately bearing
4 the burden of proof has failed to establish the existence of an element essential to their case,
5 Rule 56 mandates the entry of summary judgment against that party. *Celotex*, 477 U.S. at 322.
6 The Court should enter summary judgment against the Plaintiffs here.

7 **III. PLAINTIFFS HAVE NOT ESTABLISHED THEIR STANDING AND CANNOT**
8 **DO SO WITHOUT RISK OF GRAVE DAMAGE TO NATIONAL SECURITY.**

9 **A. Plaintiffs Have Not Carried Their Evidentiary Burden of Establishing**
10 **Their Standing.**

11 As the Government has briefed numerous times in the course of this litigation, to obtain
12 relief of any kind in this case, Plaintiffs must present “specific facts” showing that they are
13 “among the [persons] injured” by the Government’s alleged unlawful conduct. *Amnesty*
14 *International*, 133 S. Ct. at 1149; *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 563 (1992)
15 (citations and internal quotation mark omitted). That is, Plaintiffs must establish “with the
16 manner and degree of evidence” required at the summary-judgment stage that communications
17 of theirs are currently being seized and searched as part of NSA’s Upstream collection.
18 *Defenders of Wildlife*, 504 U.S. at 561. They have not done so.

19 Plaintiffs continue to assert that their communications are among those “seized” and
20 “searched” in the course of Upstream collection based on the claim that “AT&T allows the
21 [G]overnment to seize the entire communications stream of its customers,” including Plaintiffs.
22 Pls.’ Mot. at 9-10. Plaintiffs rely entirely on the eight-year-old Klein and Marcus declarations to
23 establish this essential fact. *Id.* at 6 nn. 5-8. But as discussed above, Mr. Klein lacks any
24 personal knowledge of what equipment actually resided or what activities actually occurred in
25 the “SG3 Secure Room” where he claims that copies of all or substantially all of the
26 communications transiting the peering links at AT&T’s Folsom Street facility were diverted to
27 the NSA. Mr. Marcus attests to the capabilities of equipment that documents provided by Mr.
28 Klein indicate were to be installed in the SG3 Room, but in the final analysis he, too, can only
guess at what equipment actually was in use there, its purpose, and “what entities” had access to

1 communications allegedly processed there. Moreover, both individual’s testimony is so
2 outdated—concerning events that supposedly took place in 2002 and 2003—that it lacks any
3 probative value as to ongoing activities. Because Plaintiffs have failed to adduce any admissible
4 evidence to support this “essential element of their case,” summary judgment must be awarded
5 against Plaintiffs, not for them. *Defenders of Wildlife*, 504 U.S. at 562; *Celotex*, 477 U.S. at 322.

6 At best, Plaintiffs are asking the Court to speculate that Plaintiffs’ communications are
7 among those collected today based on events that allegedly occurred over a decade ago. As the
8 Supreme Court made clear in *Amnesty International*, such speculation is an impermissible basis
9 on which to predicate Article III standing. 133 S. Ct. at 1149.

10 **B. Even if Plaintiffs Had Presented Admissible Evidence to Support**
11 **Their Standing, the State Secrets Doctrine Would Still Require Entry**
12 **of Judgment for the Government on the Standing Issue.**

13 Due to the failings of Plaintiffs’ evidence described above, the Court need not consider
14 the impact of the state secrets privilege on the standing issue. However, if the Court were to find
15 Plaintiffs’ declarations admissible and sufficiently probative of Plaintiffs’ standing to raise a
16 genuine issue meriting further inquiry (which it should not), adjudication of the standing issue
17 could not proceed without risking exceptionally grave damage to national security (a threshold
18 issue on which the Court requested briefing). That is so because operational details of Upstream
19 collection that are subject to the DNI’s assertion of the state secrets privilege in this case are
20 necessary to address Plaintiffs’ theory of standing. The Government presented this evidence to
21 the Court in the DNI’s and NSA’s classified declarations of December 20, 2013, and
22 supplements it with the Classified Declaration of Miriam P., NSA, submitted *in camera, ex*
23 *parte*, herewith. Disclosure of this evidence would risk informing our Nation’s adversaries of
24 the operational details of the NSA’s Upstream collection, including the identities of electronic-
25 communications-service providers assisting with Upstream collection. The risk of grave damage
26 to national security from disclosure of this evidence remains, notwithstanding the unauthorized
27 public disclosures and official Government releases of previously classified information about
28 certain NSA intelligence-gathering activities since June 2013. *See* Govt. Defs.’ Reply on
Threshold Legal Issues (ECF No. 185) at 18-20 (“Govt.’s Reply on Threshold Issues”).

1 Plaintiffs claim in their motion that “[n]o genuine issue of material fact exists that
2 plaintiffs’ provider AT&T is one of the Internet backbone providers at issue.” Pls.’ Mot. at 10.
3 Even if that were so, it would not be sufficient to show that Plaintiffs’ communications,
4 specifically, are subject to any alleged seizure or search involved in Upstream collection. More
5 to the point, however, the Government has already explained, in the course of the briefing on the
6 Court’s four threshold questions, that the same sources Plaintiffs point to in their instant motion
7 as proof of AT&T’s participation in Upstream collection—*e.g.*, the Klein and Marcus
8 declarations, the decision by then-Chief Judge Walker in *Hepting v. AT&T*, 439 F. Supp. 2d 974
9 (N.D. Cal. 2006), and the NSA Draft Inspector General report—do not in fact prove that AT&T
10 participates in the program or that the Government has so confirmed. Govt.’s Reply on
11 Threshold Issues at 20-24. Indeed, as held by another member of this Court in a recent case, the
12 identities of electronic-communications-service providers assisting with NSA intelligence-
13 gathering activities remain classified. *Electronic Frontier Found. v. Dep’t of Justice*, 2014 WL
14 3945646, at *5-7 (N.D. Cal. Aug. 11, 2014) (holding that identities of telecommunications-
15 service-providers participating in the NSA’s Section 215 telephony metadata program remain
16 classified, rejecting arguments that providers’ names have been officially acknowledged).

17 As the Court recognized in its July 23, 2013, decision, where evidence must be protected
18 from disclosure in the interests of national security, and that information is needed to adjudicate
19 a claim or any defenses thereto, the plaintiff’s claims must be dismissed and judgment entered
20 for the defendant. *See Kasza v. Browner*, 133 F.3d 1159, 1166 (9th Cir. 1998); *Jewel*, 965 F.
21 Supp. 2d at 1100, 1102-03. The harm to national security here cannot be abated by holding an *in*
22 *camera*, *ex parte* proceeding under 50 U.S.C. § 1806(f). As the Government explained in
23 response to the Court’s third question, because Plaintiffs base their standing on the claim that the
24 entire stream of AT&T’s communications, at least in the San Francisco area, is seized and
25 searched, any adjudication of Plaintiffs’ standing as a result of a § 1806(f) proceeding would
26 necessarily reveal whether or not AT&T participates in Upstream collection, and even more
27 specifically, whether or not AT&T’s Folsom Street facility in San Francisco is involved in
28 Upstream collection. Govt.’s Reply on Threshold Issues at 16. The Supreme Court in *Amnesty*

1 *Int'l*, 133 S. Ct. at 1149 n.4, warned against resort to an *in camera* proceeding in precisely these
2 circumstances—where “the court’s post-disclosure decision about whether to dismiss the suit for
3 lack of standing” would reveal sensitive national security information that the proceeding was
4 designed to protect. *See* Govt’s Reply on Threshold Issues at 14-16.

5 For these fundamental reasons, Plaintiffs have not established their standing to raise a
6 Fourth Amendment claim based on Upstream collection. Alternatively, even if they had
7 presented sufficient evidence of their standing to raise a genuine issue regarding their standing,
8 the question cannot be litigated without potentially harmful disclosures of privileged national-
9 security information. Plaintiffs’ motion for summary judgment must therefore be denied, their
10 claims dismissed, and judgment awarded to the Government.

11 **IV. PLAINTIFFS SHOULD BE DENIED SUMMARY JUDGMENT, AND**
12 **JUDGMENT SHOULD INSTEAD BE AWARDED TO THE GOVERNMENT,**
13 **ON THE MERITS OF PLAINTIFFS’ FOURTH AMENDMENT CLAIM.**

14 **A. Plaintiffs’ Claim of a Seizure at “Stage 1” Fails as a Matter of Fact and Law.**

15 The first of the two Fourth Amendment violations asserted by Plaintiffs is that the
16 Government unconstitutionally, through Upstream collection authorized under Section 702 (and
17 FISC orders) seizes their Internet-based communications (and those of millions of other
18 Americans) by obtaining copies automatically created and then delivered to the Government by
19 their Internet service provider, AT&T. Pls.’ Mot. at 2, 16-19. The alleged seizure occurs at what
20 Plaintiffs designate “stage one” of “the [G]overnment’s surveillance process,” where they
21 maintain the Government “taps into the Internet backbone networks of the nation’s leading
22 telecommunications carriers, including AT&T,” to obtain “access to the entire stream” of
23 Internet-based domestic and international communications. According to Plaintiffs, this alleged
24 interception and copying of the “communications stream” is “a general seizure that is not, and
25 never could be, authorized by a valid warrant.” *Id.* at 6, 16.

26 Plaintiffs’ application for summary judgment on this claim must be denied, and judgment
27 awarded instead to the Government, for two reasons: (1) Plaintiffs have adduced no admissible
28 evidence to support the contention that the NSA’s “Upstream” collection of communications
involves the interception and copying of the entire communications stream carried by AT&T (or

1 any other provider); and (2) even if Plaintiffs’ evidence—the “facts” asserted in the Klein and
2 Marcus declarations—were taken at face value, the conduct ascribed to the Government does
3 not, as a matter of law, constitute a Fourth Amendment seizure.

4 **1. Plaintiffs have presented no admissible evidence that**
5 **Upstream collection under Section 702 in fact involves**
6 **the “Stage 1” seizure they allege.**

7 As discussed above, the Government has acknowledged that pursuant to Section 702 it
8 engages in targeted “Upstream” acquisition of communications as they “transit the Internet
9 ‘backbone’” networks of telecommunications-service providers within the United States.” IC
10 Coll. Pgms. at 3; *see supra* at 6-7. The Government has not disclosed, however, the technical
11 details of the means by which providers make these targeted communications available to the
12 Government. Those operational details remain classified.

13 As support, therefore, for their allegations that the Government intercepts and copies the
14 entire communications stream from AT&T’s Internet backbone network—the very essence of
15 their seizure claim—Plaintiffs rely exclusively on the attestations of the Klein and Marcus
16 declarations. *See* Pls.’ Mot. at 6 & nn. 4-8. As discussed *supra*, § II, nothing that Messrs. Klein
17 and Marcus say about the Government’s alleged interception and copying of Internet-based
18 communications at AT&T’s Folsom Street facility constitutes admissible evidence. Moreover,
19 the information on which both declarants rely about the SG3 Secure Room in 2003 is now more
20 than a decade old, and relates to alleged events occurring years before Section 702 was enacted.
21 It is therefore not probative of any intelligence activity in which the Government *currently*
22 engages, *see supra* at 18-19—the exclusive concern, as Plaintiffs themselves state, of their
23 request for summary judgment. Pls.’ Mot. at 1. Thus, Plaintiffs have failed to adduce any
24 competent evidence that Upstream collection, or any other Government intelligence program,
25 involves the interception and copying of the entire communications stream from AT&T’s (or any
26 other provider’s) Internet backbone network, and so doing have presented no evidence to support
27 an essential element of their seizure claim as they have defined it. For this simple reason if no
28 other the Government, not Plaintiffs, is entitled to judgment on Plaintiffs’ seizure claim.
Celotex, 477 U.S. at 322.

1 **2. Even if proven, the alleged “Stage 1” splitting of the Internet**
2 **communications stream would not constitute a Fourth**
3 **Amendment seizure as a matter of law.**

4 Even if the Klein and Marcus declarations could be accepted as evidence of ongoing
5 Government conduct, the Government would still be entitled to judgment on Plaintiffs’ seizure
6 claim as a matter of law. Plaintiffs allege surveillance involving the real-time interception and
7 copying of electronic communications, without delay or interruption in their flow, followed by
8 filtering for foreignness and scanning for targeted selectors, whereupon, as discussed below, the
9 communications at issue here are destroyed within milliseconds of their creation without
10 retention by the Government. This process does not involve a seizure for which a warrant or
11 probable cause is required, because it does not constitute a Fourth Amendment “seizure” at all.

12 An evaluation of Plaintiffs’ seizure claim must begin with an understanding of what
13 constitutes a seizure for purposes of the Fourth Amendment, a subject bypassed in Plaintiffs’
14 motion. The Fourth Amendment assures the “right of the people to be secure in their persons,
15 houses, papers, and effects, against unreasonable searches and seizures.” U.S. Const. amend IV,
16 cl. 1. As the Supreme Court and the Ninth Circuit have explained, “[d]ifferent interests are
17 implicated by a seizure than by a search. A seizure affects only [a] person’s possessory interests;
18 a search affects a person’s privacy interests.” *Segura v. United States*, 468 U.S. 796, 806 (1984)
19 (citations omitted); *United States v. Jacobsen*, 466 U.S. 109, 113 (1984); *Texas v. Brown*, 460
20 U.S. 730, 747-48 (1983) (Stevens, J., concurring); *United States v. Jefferson*, 566 F.3d 928, 933
21 (9th Cir. 2009). Accordingly, a Fourth Amendment seizure of property occurs “when there is
22 some meaningful interference with an individual’s possessory interests in that property.”
23 *Jacobsen*, 466 U.S. at 113; *Jefferson*, 566 F.3d at 933. “Absent such interference, no fourth
24 amendment seizure will be found.” *DeBoer v. Pennington*, 206 F.3d 857, 865 (9th Cir. 2000)
25 (quoting *United States v. England*, 971 F.2d 419, 420 (9th Cir. 1992)). See also, e.g., *United*
26 *States v. Clutter*, 674 F.3d 980, 984-85 (8th Cir. 2012); *United States v. Va Lerie*, 424 F.3d 694,
27 708 (8th Cir. 2005) (no seizure where temporary removal of bus passenger’s checked luggage
28 during a re-fueling stop did not meaningfully interfere with his possessory interests); *United*
States v. Elmore, 304 F.3d 557, 560-61 (6th Cir. 2002); *United States v. Brown*, 884 F.2d 1309,

1 1311 (9th Cir. 1989) (“[n]o seizure occurred” when detectives arranged to have airline
2 passenger’s checked suitcases held while they obtained his permission to search them).

3 Plaintiffs do not explain what *possessory* interest they have in the “communications
4 stream”—modulated electromagnetic impulses moving at the speed of light across fiber-optic
5 networks—but it is clear no meaningful interference with any such interest occurs at Stage 1 of
6 the surveillance process they allege, which involves no interruption or delay of communications
7 they send or receive, or retention by the Government of the copied communications that
8 Plaintiffs identify as the subject of their motion.

9 Plaintiffs maintain that due to similarities between electronic communications such as
10 e-mail and traditional forms of communication such as letters and telephone calls, electronic
11 communications are entitled to similar Fourth Amendment protection. Pls.’ Mot. at 11-14. But
12 Plaintiffs do not benefit from that analogy. The Ninth Circuit, together with other courts of
13 appeals, has repeatedly held that the possessory interest protected by the Fourth Amendment in
14 mailed (or privately shipped) letters and packages is “solely in [their] timely delivery.” *United*
15 *States v. Jefferson*, 566 F.3d 928, 933-34 (9th Cir. 2009); *United States v. Hoang*, 486 F.3d 1156,
16 1160 (9th Cir. 2007). Accordingly, the Court of Appeals has held that no Fourth Amendment
17 seizure occurs unless the government’s temporary detention of a mailed letter or package, once
18 in transit, “significantly interfere[s] with [its] timely delivery in the normal course of business.”
19 *Hoang*, 486 F.3d at 1162 & nn. 2-3 (ten-minute detention of FedEx package for purpose of
20 canine narcotics sniff that did not interfere with package’s scheduled delivery did not implicate
21 the recipient’s Fourth Amendment rights) (citing, *inter alia*, *United States v. Zacher*, 465 F.3d
22 336, 338-39 (8th Cir. 2006) and *United States v. LaFrance*, 879 F.2d 1, 7 (1st Cir. 1989)); *see*
23 *also Jefferson*, 566 F.3d at 934-35 (citing *United States v. Gill*, 280 F.3d 923, 932-33 (9th Cir.
24 2002) (Gould, J., concurring)) ; *United States v. England*, 971 F.2d 419, 420-21 (9th Cir. 1992)
25 (citing *United States v. Place*, 462 U.S. 696, 718 n.5 (1983) (Brennan, J., concurring) (“mere
26 detention of mail not in [the defendant’s] custody or control amounts to at most a minimal or
27 technical interference with his person or effects, resulting in no deprivation at all”)).

1 The “Stage 1” duplication of electronic communications alleged by Plaintiffs results in no
2 demonstrated delay in the delivery of anyone’s communications; indeed, Plaintiffs themselves
3 explain that the purpose of the electronic copying that they condemn as a “seizure” is to *avoid*
4 “interrupting or slowing Internet communications” by “allow[ing] one copy of the [duplicated]
5 communications stream to travel as it normally would to its intended destination on the Internet.”
6 Pls.’ Mot. at 6; *see also* Marcus Decl. ¶¶ 62, 72-73. Thus, by Plaintiffs’ own telling, Stage 1
7 causes no delay in the communications that Plaintiffs send or receive, as would be required to
8 demonstrate a seizure under the traditional Fourth Amendment principles Plaintiffs invoke.

9 Moreover, because the communications at issue are not retained by the Government,
10 Plaintiffs’ claim is also undermined by precedent holding that no seizure takes place when law-
11 enforcement officers momentarily pick up an item or move it a short distance for the purpose of
12 a brief visual or other non-intrusive form of inspection. For example, in *United States v. Hall*,
13 978 F.2d 616 (10th Cir. 1992), a narcotics agent proceeded to the luggage area of the train on
14 which a suspected drug courier was traveling and lifted her suitcase from the bin in which it had
15 been stowed. Finding the bag suspiciously heavy, the agent detained it for an intended canine
16 sniff test and, ultimately, a search revealing 40 pounds of marijuana inside. *Id.* at 618-19. The
17 court held that the agent’s initial “lifting of [the] suitcase did not constitute a seizure because this
18 interference with [the courier’s] possessory interests in her suitcase was minimal.” *Id.* at 619. In
19 reaching this conclusion, the court relied on *Arizona v. Hicks*, 480 U.S. 321 (1987), *see Hall*, 978
20 F.2d at 619-20, where the Supreme Court held that turning over a piece of stereo equipment to
21 read and record its serial number did not “[i]n and of itself” amount to a seizure because “it did
22 not meaningfully interfere with [the defendant’s] possessory interest in either the serial number
23 or the equipment.” *Hicks*, 480 U.S. at 324 (citation and quotation marks omitted). *See also*
24 *United States v. Schofield*, 80 Fed. Appx. 798, 802-03 (3d Cir. 2003) (officer “almost certainly
25 did not seize” box by lifting it during search of car trunk); *United States v. DeMoss*, 279 F.3d
26 632, 634-36 (8th Cir. 2002) (officer did not seize passing package when he lifted it from
27 conveyor belt); *United States v. Gant*, 112 F.3d 241-42 (6th Cir. 1997); *United States v. Harvey*,
28 961 F.2d 1361, 1363-64 (8th Cir. 1992).

1 The Stage 1 copying of communications that Plaintiffs allege, for the subsequent purpose
2 of real-time filtering for foreignness and scanning to detect communications containing lawfully
3 targeted selectors, is analogous to “pick[ing] up an individual’s property to look at it,” and
4 likewise results in no seizure because “th[e] interference with the [communicant’s] possessory
5 interest” in the communication “is not meaningful.” *Hall*, 978 F.2d at 619. Plaintiffs and their
6 expert, Mr. Marcus, posit a surveillance process by which millions of Americans’ Internet-based
7 communications are copied, filtered for foreignness, and scanned for targeted selectors in “real
8 time,” at “true carrier speeds,” as those communications propel across providers’ fiber-optic
9 networks at incomprehensible speed. Pls.’ Mot. at 6-8; Marcus Decl. ¶¶ 80, 83. Ultimately
10 some of those communications (those found at Stage 3 to contain targeted selectors) are stored in
11 Government databases (at Stage 4), but that is not the “seizure” complained of; Plaintiffs
12 expressly state that “[t]he communications the [G]overnment retains at stage four are not at issue
13 here.” Pls.’ Mot. at 8-9. Rather, Plaintiffs contest the legality of the alleged seizure of those
14 communications that are not retained in Government databases (because they are not found to
15 contain targeted selectors). But because, under the scenario described by Plaintiffs, these
16 communications are copied, filtered for foreignness, and scanned for targeted selectors in real
17 time as the communications stream at the speed of light, the copies could exist for no more than
18 milliseconds before being discarded or destroyed. There is no meaningful interference with any
19 possessory interest articulated by Plaintiffs that results from the Government’s alleged
20 possession of these copied communications for literally thousandths of a second.

21 The almost instantaneous destruction of the copied communications once they are made
22 distinguishes the scenario alleged by Plaintiffs from situations where government authorities
23 obtain copies of individuals’ electronic information—such as e-mails stored on a provider’s
24 server, or data contained on a laptop computer—and retain it in government databases for
25 investigatory purposes. In such cases, some courts have held that the government’s acquisition
26 and indefinite retention of the copied data constitutes a seizure, because “an individual’s
27 possessory interest in [such data] extends to both the original and any copies made from it.” *See*,
28 *e.g.*, *In re Search of Info. Associated with [Redacted] at mac.com [etc.]*, 2014 WL 1377793, at

1 *2, 3 (D.D.C. Apr. 7, 2014), *vacated on other grounds*, 2014 WL 4094565 (D.D.C. Aug. 8,
2 2014); *United States v. Saboonchi*, 990 F. Supp. 2d 536, 565 (D. Md. 2014). In other such
3 cases, courts have held that no seizure occurs because although the government has obtained a
4 copy, the original dataset remains accessible to the owner and as a result no meaningful interest
5 with his or her possessory interest results. *See, e.g., In re Application of the United States of*
6 *America for a Search Warrant for Contents of Electronic Mail [etc.]*, 665 F. Supp. 2d 1210,
7 1222 (D. Or. 2009); *United States v. Gorshkov*, 2001 WL 1024026, at *3 (W.D. Wash. May 23,
8 2001) (citing *Hicks*, 480 U.S. at 324). But regardless of which view the law ultimately
9 embraces, the situation alleged by Plaintiffs here is materially different from these cases, because
10 they have specified that their claim concerns copies of communications data that the Government
11 does not retain, and which, once created, are almost immediately destroyed. Plaintiffs identify
12 no meaningful interference with their possessory interest in these copied communications that
13 could possibly occur during the vanishingly brief moment of their existence. The copying of
14 communications data that allegedly occurs at Stage 1 is therefore not a seizure.

15 **3. No authority cited by Plaintiffs supports their seizure claim.**

16 For their part, Plaintiffs cite no authority to support the proposition that Upstream
17 collection involves a seizure of their online communications. First they attempt to equate the
18 alleged electronic copying of a communications data stream with general warrants and writs of
19 assistance, the historic instruments of British oppression that the Fourth Amendment was most
20 urgently intended to prohibit. *See Virginia v. Moore*, 553 U.S. 164, 168-69 (2008); Pls.' Mot. at
21 17-18. As the Supreme Court has summarized their history, general warrants were employed by
22 the British Crown to authorize the arrest of all persons suspected of authoring, printing, or
23 distributing seditious publications, together with the seizure of all their personal papers; writs of
24 assistance were issued in pre-revolutionary times to give British officers blanket authority to
25 barge into colonists' homes in unrestrained search for illegally imported goods. *See Stanford v.*
26 *Texas*, 379 U.S. 476, 481-82 (1965); *Marcus v. Search Warrants of Property*, 367 U.S. 717, 726-
27 29 (1961); *see also Riley v. California*, 134 S. Ct. 2473, 2494 (2014). No amount of argument
28 on Plaintiffs' part can succeed in equating the installation of fiber-optic splitters on

1 telecommunications cables far removed from Plaintiffs' homes, to create copies of electronic
 2 data that are then almost instantaneously destroyed, as the legal equivalent of these historic
 3 offenses against personal liberty.⁶

4 There are likewise no valid parallels to be drawn between the transitory creation and
 5 destruction of copied communications at Stage 1 with the entry upon the defendants' places of
 6 business and the physical seizures (and retention) of all their business records in *United States v.*
 7 *Tamura*, 694 F.2d 591, 594-95, 596-97 (9th Cir. 1982) and *United States v. Kow*, 58 F.3d 423,
 8 425 (9th Cir. 1995). See Pls.' Mot. at 17. Alleged Stage 1 copying of the communications
 9 stream does not involve the wholesale physical confiscation from Plaintiffs' possession of their
 10 personal papers or business records, but at best a fleeting grasp and release of electronic data
 11 transiting distant fiber-optic cables, without impeding the journeys of Plaintiffs' communications
 12 to their intended destinations on the global communications network. As the process described
 13 by Plaintiffs results in no meaningful interference with any possessory interest Plaintiffs have in
 14 their electronic communications, it is not a Fourth Amendment seizure and requires neither a
 15 warrant, nor individualized suspicion.⁷

18 ⁶ The fact that the data actually retained by the Government are "not at issue here," Pls.'
 19 Mot. at 9, also eliminates any valid basis for comparing Stage 1 of the alleged surveillance
 20 process here to the NSA's Cold War-era "Operation Shamrock," or for Plaintiffs' continued
 21 reliance on this Court's prior decision in *Hepting v. AT&T*, 439 F. Supp. 2d 974 (N.D. Cal.
 22 2006), *id.* at 16-17, 18. See Intelligence Activities: Hrgs. Before the Sen. Select Comm. To
 23 Study Governmental Operations With Respect to Intelligence Activities, 94th Cong., Vol. V, 57-
 24 59 (1975) (statement that during Operation Shamrock NSA acquired and NSA analysts sorted
 through most international telegrams originating in or forwarding through the United States),
 available at http://www.intelligence.senate.gov/pdfs94th/94intelligence_activities_V.pdf;
Hepting, No. 3:06-cv-00672-VRW, First Amended Compl. ¶¶ 42-46 (ECF No. 8) (alleging that
 all or substantially all of the communications transmitted through AT&T's key domestic
 telecommunications facilities were actually acquired by the Government).

25 ⁷ Plaintiffs confuse the issue when they assert, in support of their seizure claim, that they
 26 have a reasonable expectation of privacy in the copied communications. Pls.' Mot. at 17. By
 27 definition, the violation of an individual's reasonable expectation of privacy constitutes a search,
 28 not a seizure, *see Segura*, 468 U.S. at 806; *Jacobsen*, 466 U.S. at 113, but Plaintiffs do not
 contend that electronic copying of their communications in and of itself constitutes a search.
 Rather, Plaintiffs contend that the alleged duplication of the communications stream is a seizure,
 which requires a meaningful interference with a possessory interest. Plaintiffs' reliance on
Florida v. Jardines, 133 S. Ct. 1409 (2013), and *United States v. Jones*, 132 S. Ct. 945 (2012),
see Pls.' Mot. at 17, suffers from the same confusion, as both are "search," not "seizure" cases.

1 **B. Plaintiffs' Claim That Alleged "Stage 3" Scanning Constitutes a Search**
2 **of Communications Not Found To Contain Targeted Selectors Is Also**
3 **Without Merit.**

4 Plaintiffs' second contention is that scanning copied communications at "Stage 3" (after
5 they are filtered for foreignness) for those that contain targeted selectors constitutes a Fourth
6 Amendment search. Pls.' Mot. at 19-21. In contrast to a seizure, which involves governmental
7 interference with a possessory interest, a Fourth Amendment search occurs when the government
8 obtains information by physically intruding on a constitutionally protected area, or by violating a
9 person's reasonable expectation of privacy. *Jardines*, 133 S. Ct. at 1414; *Jones*, 132 S. Ct. at
10 949-50. Plaintiffs devote a great deal of effort to establishing that they have a reasonable
11 expectation of privacy in their Internet-based communications. Pls.' Mot. at 11-14. One need
12 not quarrel with the proposition to conclude, nonetheless, that no search of Plaintiffs' online
13 communications has been demonstrated. Where the official conduct complained of "does not
14 'compromise any legitimate interest in privacy' [it] is not a search subject to the Fourth
15 Amendment." *Illinois v. Caballes*, 543 U.S. 405, 408 (2005) (quoting *Jacobsen*, 466 U.S. at
16 123). That is the case here so far as the communications at issue are concerned.

17 As discussed *supra*, at 28, Plaintiffs and their expert describe Upstream collection as a
18 process by which millions of communications are copied, filtered for foreignness and scanned
19 for targeted selectors in real time, through the use of sophisticated electronic equipment capable
20 of processing large volumes of communications data to identify "traffic of interest." Pls.' Mot.
21 at 6-8; Marcus Decl. ¶¶ 79-85. Only afterward, at "Stage 4," are the results of this filtering and
22 scanning allegedly "deposited into [G]overnment databases for retention" and "actual human
23 scrutiny." Pls.' Mot. at 8; Marcus Decl. ¶ 39. But the copied communications retained at
24 Stage 4 are "not at issue," *id.* at 9; the only copied communications at issue are those discarded,
25 within milliseconds of their creation, because they are not found as a result of the electronic
26 scanning to contain targeted selectors. Plaintiffs do not allege, much less do they submit
27 admissible evidence to prove, that any information about these discarded communications,
28 including communications of theirs, is provided to Government officials before they are
destroyed. They do not explain, for that matter, how Government personnel could know even of

1 the existence of any communications in which Plaintiffs or any other U.S. persons engage if they
2 are not among the targeted communications retained at Stage 4.

3 In this respect—that is, the utter lack of information made available to Government
4 personnel—the alleged scanning of unretained communications resembles the narcotics-dog sniff
5 of luggage, and the chemical field test for cocaine, that the Supreme Court held did not constitute
6 Fourth Amendment searches in *United States v. Place*, 462 U.S. 696, 706-07 (1983) and
7 *Jacobsen*, 466 U.S. at 123-24, respectively. In *Place*, DEA agents, suspecting an airline
8 passenger of transporting illegal narcotics, took his luggage from his possession and transported
9 his bags to another location for a “sniff test” by a trained narcotics-detection dog. The dog
10 alerted to one of the bags, after which the agents, upon obtaining a search warrant, opened the
11 bag and discovered more than a kilogram of cocaine inside. 462 U.S. at 698-99. Although
12 ultimately concluding that *Place*’s luggage had been unconstitutionally seized, the Supreme
13 Court first concluded that subjecting the luggage to the canine sniff test did not constitute a
14 search within the meaning of the Fourth Amendment. The Court explained:

15 A “canine sniff” by a well-trained narcotics detection dog . . . does not require
16 opening the luggage. *It does not expose noncontraband items that otherwise*
17 *would remain hidden from public view*, as does, for example, an officer’s
18 rummaging through the contents of the luggage. Thus, the manner in which
19 information is obtained through this investigative technique is much less intrusive
20 than a typical search. Moreover, the sniff discloses only the presence or absence
21 of narcotics, a contraband item. Thus, despite the fact that the sniff tells the
22 authorities something about the contents of the luggage, the information obtained
23 is limited. This limited disclosure also ensures that the owner of the property is
24 not subjected to the embarrassment and inconvenience entailed in less
25 discriminate and more intrusive investigative methods.

26 *Id.* at 707 (emphasis added).

27 The Court extended the logic of *Place* to a chemical test for narcotics in *Jacobsen*. In
28 that case, employees of a private freight carrier, upon discovering a white powdery substance
inside a damaged package, summoned federal narcotics agents. Upon arriving, the agents made
an “on the spot” chemical field test that identified the substance as cocaine, leading to the arrest
and conviction of the package’s intended recipients. *Jacobsen*, 466 U.S. at 111-12 & n.1. The
Court held that the chemical test did not constitute a Fourth Amendment search, because it
“could disclose only one fact . . . whether or not a suspicious white powder was cocaine”—

1 “nothing more”—and therefore “d[id] not compromise any legitimate interest in privacy.” *Id.* at
2 122-23. “[E]ven if the results are negative,” the Court emphasized, “such a result reveals
3 nothing of special interest.” *Id.* at 123. The Court observed further that its conclusion was
4 “dictated” by the decision in *Place*, because the chemical test, like a narcotics-dog sniff, “could
5 reveal nothing about noncontraband items.” *Id.* at 123-24 & n.24.

6 The logic underlying the decisions in *Jacobsen* and *Place* applies equally to Stage 3
7 scanning of communications that do not contain targeted selectors. So far as Plaintiffs maintain
8 or prove, electronic scanning at Stage 3 of communications that are not found to contain targeted
9 selectors results in their immediate destruction, without revealing anything about them to the
10 Government. Indeed, the information gleaned about unretained communications is even less
11 than the modicum of information revealed either by the canine sniff in *Place* or the chemical
12 field test in *Jacobsen*. As the Court observed in *Place*, if the narcotics-detection dog does not
13 alert, that “tells the authorities something about the contents of the luggage” (the absence of
14 illegal drugs) but that information is too “limited” to raise the intrusion to the level of a search.
15 462 U.S. at 707. Likewise, a negative chemical field test reveals “that [a] substance is something
16 other than cocaine,” but that disclosure, too, is of insufficient “interest” to result in a search.
17 *Jacobsen*, 466 U.S. at 123. Here, so far as Plaintiffs’ evidence indicates, if Stage 3 scanning of a
18 copied communication is negative the Government learns nothing about it—not even that it
19 exists. Accordingly, so far as Plaintiffs’ motion concerns only communications that have not
20 been found to contain targeted selectors, they have not shown that Government personnel obtain
21 any information about Plaintiffs’ communications, the contents thereof, or with whom Plaintiffs
22 communicate online. Thus, under the rationales of *Place* and *Jacobsen*, Plaintiffs have made no
23 showing that Stage 3 scanning of their communications “compromise[s] any legitimate interest
24 [of theirs] in privacy,” *Caballes*, 543 U.S. at 408 (quoting *Jacobsen*, 466 U.S. at 123), and so
25 have not demonstrated the occurrence of a Fourth Amendment search.

26 Plaintiffs seek to support the opposite conclusion by again invoking historic memory of
27 general warrants and writs of assistance, likening the electronic scanning of communications
28 data copied from fiber-optic cables to a “general exploratory rummaging” of every colonist’s

1 home by British troops. Pls.’ Mot. at 20-21. The comparison is ill-conceived, however, and its
 2 logical flaw is exposed by the Court’s reasoning in *Place*. There the Court explained that a
 3 narcotics-dog sniff is distinguishable from “an officer’s rummaging through the contents of [an
 4 individual’s] luggage,” because a sniff test does not expose items, other than targeted narcotics,
 5 “that otherwise would remain hidden from public view.” 462 U.S. at 707. Thus “the owner of
 6 the property is not subjected to the embarrassment and inconvenience entailed in less
 7 discriminate and more intrusive investigative methods.” *Id.* As in *Place*, communications not
 8 found at Stage 3 to contain targeted selectors “remain hidden,” so far as Plaintiffs have
 9 demonstrated, from the Government’s view, *id.*, and no search of those communications, much
 10 less the equivalent of a house-to-house search of the entire thirteen colonies, takes place. The
 11 Government, not Plaintiffs, is entitled to judgment on Plaintiffs’ search claim as a matter of law.

12 **C. The “Stage 1” Seizure and “Stage 3” Search Alleged by Plaintiffs Fall Within**
 13 **the Fourth Amendment’s “Special Needs” Doctrine and Are Reasonable**
 14 **Under the Totality of the Circumstances.**

15 Even if the alleged real-time copying and scanning of Plaintiffs’ electronic
 16 communications at Stages 1 and 3 constituted seizures and searches within the meaning of the
 17 Fourth Amendment, these activities serve special Government needs and, therefore, under settled
 18 doctrine, do not require a warrant. They are reasonable under the totality of the circumstances—
 19 reflecting Congress’s and the Executive’s careful balancing of the relevant national-security and
 20 privacy interests—and are therefore constitutional, because their importance to national security
 21 far outweighs any minimal intrusion they impose on Plaintiffs’ Fourth Amendment interests.

22 **1. The challenged surveillance activities do not require the issuance**
 23 **of a warrant upon probable cause because the Government has a**
 24 **“special need” to collect foreign-intelligence information.**

25 Plaintiffs argue that the alleged Stage 1 copying and Stage 3 scanning of their
 26 communications violate the Fourth Amendment because “[n]ational security does not excuse
 27 the need for a warrant” to conduct these activities. Pls.’ Mot. at 14. But under the Supreme
 28 Court’s “special needs” doctrine, it does. The “touchstone” of Fourth Amendment analysis “is
 always ‘the reasonableness in all the circumstances of the particular governmental invasion of a
 citizen’s personal security.’” *Pennsylvania v. Mimms*, 434 U.S. 106, 108-09 (1977) (per curiam)

1 (quoting *Terry v. Ohio*, 392 U.S. 1, 19 (1968)). “[A]lthough ‘both the concept of probable cause
 2 and the requirement of a warrant bear on the reasonableness of a search,’” *New Jersey v. T.L.O.*,
 3 469 U.S. 325, 340 (1985) (citation omitted), “neither a warrant nor probable cause, nor, indeed,
 4 any measure of individualized suspicion, is an indispensable component of reasonableness in
 5 every circumstance,” *National Treas. Emp. Union v. Von Raab*, 489 U.S. 656, 665 (1989). In
 6 fact, “the traditional probable-cause standard may be unhelpful” when the Government “seeks to
 7 prevent” dangers to public safety. *Id.* at 668.

8 The Supreme Court has recognized exceptions to the warrant requirement in a variety of
 9 circumstances, including where “special needs, beyond the need for law enforcement, make the
 10 warrant and probable-cause requirement impracticable,” *Griffin v. Wisconsin*, 483 U.S. 868, 873
 11 (1987), and the needs are motivated “at [a] programmatic level” by other governmental
 12 objectives. See *City of Indianapolis v. Edmond*, 531 U.S. 32, 37-40, 48 (2000). Under the
 13 “special needs” doctrine, the Fourth Amendment instead requires courts to “employ[] a
 14 balancing test that weigh[s] the intrusion on the individual’s [constitutionally protected]
 15 interest[s]” against the “‘special needs’ that support[] the program.” *Ferguson v. City of*
 16 *Charleston*, 532 U.S. 67, 78 (2001).⁸

17 A number of courts have held that the Government’s “special need” for foreign-
 18 intelligence information justifies an exception to the warrant requirement. See, e.g., *United*
 19 *States v. Duka*, 671 F.3d 329, 340-45 (3d Cir. 2011); *In re Directives*, 551 F.3d 1004, 1010-12,
 20 (FISC Ct. Rev. 2008); *United States v. Truong Dinh Hung*, 629 F.2d 908, 912-16 (4th Cir. 1980);
 21 *United States v. Mohamud*, 2014 WL 2866749, at *15-18 (D. Or. June 24, 2014); Cf. *United*
 22 *States v. Buck*, 548 F.2d 871, 875 (9th Cir. 1977) (“Foreign security wiretaps are a recognized
 23 exception to the general warrant requirement . . .”).

24 The rationale for these decisions derives from *United States v. U.S. Dist. Court (Keith)*,
 25 407 U.S. 297, 322 (1972), a case involving electronic surveillance for domestic security

26
 27 ⁸ Under the “special needs” doctrine, the Supreme Court has permitted warrantless stops
 28 at roadblocks to secure borders, *United States v. Martinez-Fuerte*, 428 U.S. 543, 566-67 (1976),
 warrantless searches of probationers’ homes to ensure compliance with probation conditions,
Griffin, 483 U.S. at 872-75, and warrantless searches of public school students to enforce school
 rules, *T.L.O.*, 469 U.S. at 340.

1 purposes, *id.* at 299. Although the Supreme Court there held that “prior judicial approval” was
 2 required for “the type of domestic security surveillance” at issue in that case, *id.* at 324, the Court
 3 recognized that, due to the significant differences between national-security investigations and
 4 ordinary criminal investigations, different standards for intelligence surveillance “may be
 5 compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate
 6 need of Government for intelligence information and the protected rights” of citizens. *See id.* at
 7 322-23; *Duka*, 671 F.3d at 339-41. The courts that have since addressed the issue of whether the
 8 collection of foreign-intelligence information requires a warrant—an issue the Supreme Court
 9 specifically reserved, *Keith*, 407 U.S. at 308, 322-23—have expressly distinguished *Keith*’s facts
 10 in holding that it does not. *See In re Directives*, 551 F.3d at 1010; *In re Sealed Case*, 310 F.3d
 11 717, 744 (FISA Ct. Rev. 2002); *Truong*, 629 F.2d at 913. *Cf. Clapper v. Amnesty Int’l USA*, 133
 12 S. Ct. 1138, 1143 (2013) (noting that *Keith* “implicitly suggested that a special framework for
 13 foreign intelligence surveillance might be constitutionally permissible”).⁹

14 In concluding that no warrant is required in this context, the courts have emphasized the
 15 importance of the national interest in foreign-intelligence gathering above and beyond garden-
 16 variety law enforcement, as well as the need for flexibility in the timely collection of
 17 intelligence, given the particular nature and objectives of foreign-intelligence collection. *See*
 18 *Duka*, 671 F.3d at 341; *In re Directives*, 551 F.3d at 1010-11; *Truong*, 629 F.2d at 912-14 (4th
 19 Cir. 1980); *[Redacted Caption]*, 2011 WL 10945618, at *24 (F.I.S.C. Oct. 3, 2011); *Mohamud*,
 20 2014 WL 2866749, at *16-18. Indeed, both the FISC and a district court of this Circuit have so
 21 held in cases, like this one, involving intelligence collection under Section 702. *See Mohamud*,
 22 2014 WL 2866749, at *1, 14-18; *[Redacted Caption]*, 2011 WL 10945618, at *24.

23 This Court should reach the same result, for the same reasons. A “significant purpose” of
 24 acquisitions under Section 702 must be, according to the statute’s terms, “to obtain foreign
 25 intelligence information,” 50 U.S.C. § 1881a(g)(2)(A)(v), such as information acquired to protect
 26 the Nation against foreign attacks, international terrorism, international proliferation of weapons

27 ⁹ Plaintiffs’ reliance (Pls.’ Mot. at 13, 15-17, 23, 25) on *Keith* and *Berger v. New York*,
 28 388 U.S. 41 (1967), is thus misplaced because the former involves the Fourth Amendment
 standard for electronic surveillance in a domestic-security case, *Keith*, 407 U.S. at 324, and the
 latter involves the standard for an ordinary criminal case, *Berger*, 388 U.S. at 43 & n.1, 62-64.

1 of mass destruction, and clandestine intelligence activities of foreign intelligence services. *See*
2 *id.* § 1801(e); *see also In re Directives*, 551 F.3d at 1011 (PAA, the predecessor to the FAA, had
3 the “stated purpose” of “garnering foreign intelligence” and “[t]here [was] no indication that the
4 collections of information [were] primarily related to ordinary criminal-law enforcement
5 purposes”). *Cf. In re Sealed Case*, 310 F.3d at 745-46 (“programmatic purpose” of obtaining
6 foreign intelligence was “a special need”); *Cassidy v. Chertoff*, 471 F.3d 67, 82 (2d Cir. 2006)
7 (interest in preventing terrorist attacks goes “well beyond” law enforcement). Plaintiffs make no
8 serious argument that Upstream collection is undertaken for routine law enforcement or any
9 purpose other than furthering “legitimate national security concerns.” Pls.’ Mot. at 25.¹⁰

10 Upstream collection also meets the impracticability requirement of the special-needs
11 doctrine. Congress, in fact, authorized the surveillance activities challenged here by enacting the
12 FAA in 2008 “with a bipartisan majority” and “broad support from the intelligence community.”
13 H.R. Rep. No. 112-645(I), 112th Cong., 2d Sess., at 2 (Aug. 2, 2012), in part because the
14 burdens imposed on the Government’s limited intelligence resources and the delays occasioned
15 by the requirement under then-current law to prepare individualized, probable-cause FISA
16 applications for intelligence collection targeting non-U.S. persons outside the United States were
17 undermining the Government’s ability to collect such information. *See* 154 Cong. Rec. S6097,
18 S6122 (daily ed., June 25, 2008) (statement of Senator Chambliss) (“[T]he [FAA] will fill the
19 gaps identified by our intelligence officials and provide them with the tools and flexibility they
20 need to collect intelligence from targets overseas.”); May 1, 2007 FISA Mod. Hrg., *supra*, at 18
21 (testimony of DNI explaining “massive amounts of analytic resources [required] to craft FISA
22 applications” for warrants authorizing collection of the communications of non-U.S. persons
23

24 ¹⁰ Plaintiffs do quarrel, however, that collection under Section 702 does not meet the
25 requirements of the special-needs exception because first, the category of foreign intelligence
26 includes “information that relates to national defense” and “foreign affairs,” and second, because
27 obtaining foreign intelligence need only be a “significant purpose” of an acquisition rather than
28 its primary purpose. Pls.’ Mot. at 25 n.24, citing 50 U.S.C. §§ 1801, 1881a(g)(2)(A)(v). But
national defense and foreign affairs are Government interests just as unrelated to routine law
enforcement as counter-terrorism. And, so long as the Section 702 program serves the
Government’s need to obtain foreign intelligence, it does not render the warrant requirement any
less impracticable, or render the special-needs exception inapplicable, just because the program
also promotes other legitimate governmental interests. *See, e.g., Duka*, 671 F.3d at 341-45; *In re*
Directives, 551 F.3d at 1011; *Mohamud*, 2014 WL 2866749, at *18.

1 located abroad); *see also* H.R. Rep. No. 112-645(II), 112th Cong., 2d Sess., at 2 (Aug. 2, 2012)
 2 (technological changes had made FISA “impractical” and “ineffective” in “combatting the
 3 quickly evolving threats facing our nation,” whereas the FAA provided “the speed and agility
 4 necessary to meaningfully collect foreign intelligence”).¹¹

5 The courts have also long recognized that “attempts to counter foreign threats to the
 6 national security require the utmost stealth, speed, and secrecy,” *Truong*, 629 F.2d at 913, and
 7 that conditioning acquisitions of foreign-intelligence information targeted at non-U.S. persons
 8 located overseas on obtaining a warrant “would add a procedural hurdle that would reduce the
 9 flexibility of executive foreign intelligence initiatives, in some cases delay executive response to
 10 foreign intelligence threats,” *id.*, “hinder the government’s ability to collect time-sensitive”
 11 foreign intelligence, and thus “impede the vital national security interests that are at stake.” *In re*
 12 *Directives*, 551 F.3d at 1011; *see also United States v. Bin Laden*, 126 F. Supp. 2d 264, 273
 13 (S.D.N.Y. 2000) (“imposition of a warrant requirement [would] be a disproportionate and
 14 perhaps even disabling burden” on Government’s ability to obtain foreign intelligence
 15 information). Courts considering the issue have found, in particular, that “application of the
 16 warrant requirement would [also] be impracticable” for acquisitions under Section 702.
 17 *Mohamud*, 2014 WL 2866749, at *18; *see also [Redacted Caption]*, 2011 WL 10945618, at *24.

18 Accordingly, the alleged seizure and search about which Plaintiffs complain fall under
 19 the Fourth Amendment’s “special needs” exception to the warrant requirement.

20
 21 **2. The challenged “Stage 1” copying and “Stage 3” scanning of**
 22 **Plaintiffs’ unretained communications are reasonable because**
 23 **the interests of national security far outweigh the minimal**
 24 **intrusion on Plaintiffs’ Fourth Amendment interests.**

25 Even where a warrant and probable cause are not required, searches and seizures remain
 26 subject to the Fourth Amendment’s “traditional standards of reasonableness.” *Maryland v. King*,
 27 133 S. Ct. 1958, 1970 (2013). In assessing the reasonableness of the putative “seizure” and
 28 “search” at Stages 1 and 3, the Court must consider the “totality of the circumstances,” *Samson*

¹¹ The Senate Select Committee on Intelligence similarly concluded in 2012 that, without
 Section 702 (and the other authorities granted by the FAA) the Intelligence Community’s
 “ability . . . to respond quickly to new threats and intelligence opportunities” would be
 “impede[d].” S. Rep. No. 112-174, 112th Cong., 2d Sess., at 2 (June 7, 2012).

1 *v. California*, 547 U.S. 843, 848 (2006), weighing “the promotion of legitimate governmental
2 interests against the degree to which [the seizures and searches] intrude[] upon” Plaintiffs’
3 protected Fourth Amendment interests. *King*, 133 S. Ct. at 1970. Applying this test, the FISA
4 Court of Review found foreign-intelligence collection under the PAA reasonable, *In re*
5 *Directives*, 551 F.3d 1012-15, and the *Mohamud* court recently found reasonable (and thus
6 constitutional) the acquisition of foreign intelligence under Section 702, *see Mohamud*, 2014 WL
7 2866749, at *19-27. This Court, likewise, should conclude that the claimed seizure and search at
8 issue here are reasonable; indeed, they infringe upon Fourth Amendment interests to a far lesser
9 degree than the intelligence-gathering activities upheld in *In re Directives* and *Mohamud*.

10 The Government’s national-security interest in conducting acquisitions pursuant to
11 Section 702 “is of the highest order of magnitude.” *In re Directives*, 551 F.3d at 1012;
12 [Redacted caption], 2011 WL 10945618, at *25 (same). “[N]o governmental interest is more
13 compelling than the security of the Nation,” *Haig v. Agee*, 453 U.S. 280, 307 (1981), and
14 combatting international terrorism, one of the principal goals of the FAA of 2008, *see* H.R. Rep.
15 No. 112-645(I), 112th Cong., 2d Sess., at 4 (Aug. 2, 2012), “is an urgent objective of the highest
16 order.” *Holder v. Humanitarian Law Project*, 561 U.S. 1, 28 (2010).

17 To be weighed against the promotion of the compelling Government interest in protecting
18 national security is the minimal intrusion on Plaintiffs’ Fourth Amendment interest by Upstream
19 collection as Plaintiffs allege it operates. As explained *supra*, §§ IV.A and B, the temporary
20 creation of a copy of Plaintiffs’ communications and the equally fleeting electronic scanning of
21 communications not retained by the Government, and about which Government personnel obtain
22 no information, produce a minimal intrusion, if any, on Plaintiffs’ possessory and privacy
23 interests, not the “massive[] intru[sion]” Plaintiffs claim. Pls.’ Mot. at 24.

24 Any intrusion on Plaintiffs’ Fourth Amendment interests is diminished further because
25 “[s]urveillance under [Section 702] is subject to statutory conditions, judicial authorization,
26 congressional supervision, and compliance with the Fourth Amendment,” *Amnesty Int’l USA*,
27 133 S. Ct. at 1144, and this “matrix of [statutory] safeguards,” *In re Directives*, 551 F.3d at 1013,
28 contributes further to the program’s reasonableness. *See Mohamud*, 2014 WL 2866749, at *27;

1 *cf. King*, 133 S. Ct. at 1979-80 (statutory protections guarding against further invasion of privacy
 2 contribute to reasonableness). The statute requires the DNI and the Attorney General to certify,
 3 and the FISC to approve, that a significant purpose of an acquisition is to obtain foreign
 4 intelligence information, *id.* § 1881a (g)(2)(A)(v), (i). Section 702 also requires the DNI and the
 5 Attorney General annually to certify—and the FISC to so find—that acquisitions will comply
 6 with the Fourth Amendment and the statutorily required targeting procedures are reasonably
 7 designed to target only non-U.S. persons reasonably believed to be located outside the United
 8 States, that is, those who do not have Fourth Amendment rights, *United States v. Verdugo-*
 9 *Urquidez*, 494 U.S. 259, 271 (1990). *See* 50 U.S.C. § 1881a(a), (b), (d)(2), (g), (i).¹² Along
 10 with the Executive’s reports to the FISC and to Congress about “compliance with the targeting
 11 . . . procedures,” *id.* § 1881a(l)(1), these requirements contribute to the reasonableness of the
 12 collection under Section 702. *See Mohamud*, 2014 WL 2866749, at *27.¹³

13 The Fourth Amendment requires only that the acquisitions of intelligence made possible
 14 by the alleged seizures and searches at issue here be a “reasonably effective means” of advancing
 15 the Government’s goals of protecting the Nation’s security. *Board of Educ. of Independent Sch.*
 16 *Dist. No. 92 of Pottawatomie County v. Earls*, 536 U.S. 822, 837-38 (2002). There should be no
 17 dispute here that this standard has been met and exceeded because the collection authorized by
 18 Section 702, the “primary surveillance authority granted by” the FAA, S. Rep. No. 112-229,
 19 112th Cong., 2d Sess., at 4 (Sept. 20, 2012), has been critical to the Government’s efforts to

20 _____
 21 ¹² Plaintiffs are wrong to complain that the “Executive alone makes all [the] decisions”
 22 about targeting “without judicial oversight,” Pls.’ Mot. at 23, because the statute imposes
 23 significant limitations on permissible targeting and the purposes for which information may be
 24 collected, 50 U.S.C. § 1881a(b), (g)(2)(A)(v), and compliance with those limitations is reviewed
 25 by the FISC. *See id.* § 1881a(i); PCLOB Report at 26-28 (describing FISC’s role as “extensive”
 26 in some respects). They are also wrong in dismissing the FISC’s role in the process as that of
 27 “an administrative agency” instead of an Article III court. Pls.’ Mot. at 21-22. The FISC
 28 determines whether the Executive is complying with the statutory requirements and the Fourth
 Amendment, *see* 50 U.S.C. § 1881a(i), and issues orders either approving of certifications (so
 directives may be issued to electronic communication service providers who must comply or
 challenge them, *see id.* § 1881a(h)), or disapproving the certifications so the Government is
 barred from conducting collections under the certifications if it does not remedy the deficiency.
Id. § 1881a(i)(2). *See Mohamud*, 2014 WL 2866749, at *10-11.

¹³ *Cf. Amnesty Int’l, USA*, 133 S. Ct. at 1150 (noting importance of requirement that the
 FISC “assess whether the Government’s targeting and minimization procedures comport with the
 Fourth Amendment”); *In re Directives*, 551 F.3d at 1015 (minimization procedures reduce
 impact of any potential privacy intrusions).

1 combat international terrorism and other threats to the United States and its interests abroad. *See*
 2 S. Rep. No. 112-174, 112th Cong., 2d Sess., at 2 (June 7, 2012) (describing collections under the
 3 FAA as “critical”); H.R. Rep. No. 112-645(I), 112th Cong., 2d Sess., at 2 (Aug. 2, 2012) (FAA
 4 authorities “critical” and “allow[] intelligence professionals to more quickly and effectively
 5 monitor terrorist communications”); H.R. Rep. No. 112-645(II), 112th Cong., 2d Sess., at 3 (Aug.
 6 2, 2012) (emphasizing “critical import[ance]” of the FAA).

7 In recommending re-authorization of the FAA in 2012, for example, the House
 8 Committee on Intelligence, which “held two hearings and multiple classified briefings” on the
 9 efficacy of surveillance under the FAA, found that the:

10 importance of the collection of foreign intelligence under the [FAA] . . . cannot be
 11 underscored enough. In short, intelligence collected under the FAA is critically
 12 important to maintaining our national security. The information collected under
 13 this authority is often unique, unavailable from any other source, and regularly
 provides critically important insights and operationally actionable intelligence on
 terrorists and foreign intelligence targets around the world.

14 H.R. Rep. No. 112-645(II), 112th Cong., 2d Sess., at 3, 5 (Aug. 2, 2012); *see also* PCLOB
 15 Report at 124 (finding that Upstream collection “has unique value”). Similarly, the Senate Select
 16 Committee on Intelligence found—based on “numerous hearings” and years of briefings by
 17 Executive Branch officials—that “the authorities provided under the [FAA] have greatly
 18 increased the government’s ability to collect information and act quickly against important
 19 foreign intelligence targets.” S. Rep. No. 112-174, 112th Cong., 2d Sess., at 2 (June 7, 2012).¹⁴

20 The Executive Branch’s assessment of the value and importance of intelligence-gathering
 21 activities authorized under the FAA is “entitled to deference.” *Humanitarian Law Project*, 561
 22 U.S. at 32-34. On a daily basis the Executive Branch confronts an array of constantly evolving
 23 threats to national security, and is charged with making difficult judgments about how best to
 24 counter those threats. *See id.*; *Truong*, 629 F.2d at 914 (Executive has “superior expertise” in

25 _____
 26 ¹⁴ Indeed, even those members of the House Judiciary Committee who “strongly
 27 oppose[d]” reauthorization, H.R. Rep. No. 112-645(I), 112th Cong., 2d Sess., at 13 (Aug. 2,
 28 2012) (dissenting views), recognized “[w]ithout question” that the FAA provided the intelligence
 community with an “important tool” to “collect significant and valuable foreign intelligence.”
Id. at 17 (dissenting views). The same was true of the minority views expressed in the report by
 the House Permanent Select Committee on Intelligence. *See* H.R. Rep. No. 112-645(II), 112th
 Cong., 2d Sess., at 10 (Aug. 2, 2012) (minority views).

1 foreign intelligence and is “constitutionally designated as the pre-eminent authority in foreign
2 affairs”). Congress’s judgment regarding the value and importance of intelligence acquisitions
3 authorized under the FAA, as reflected in its 2012 reauthorization of these authorities—including
4 Section 702—*see* FISA Amendments Act Reauthorization Act of 2012, Pub. L. No. 112-238,
5 126 Stat. 1631, is also entitled to the courts’ respect. *Humanitarian Law Project*, 561 U.S. at 33-
6 35; *see also Jones*, 132 S. Ct. at 964 (Alito, J., concurring in the judgment) (“A legislative body
7 is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy
8 and public safety in a comprehensive way.”).¹⁵

9 Each court to consider the question has concluded that the Government’s compelling
10 interest in protecting national security justifies the arguably greater intrusion of electronic
11 surveillance under Section 702, and its predecessor, the PAA, on the privacy of those individuals
12 whose electronic communications are, in fact, retained by the Government and are subject to
13 further review and scrutiny by Government officials. *See In re Directives*, 551 F.3d at 1012-16
14 (finding that the PAA, which authorized surveillance of U.S. persons abroad (and was thus
15 broader than the FAA), “constitute[d] a sufficiently reasonable exercise of governmental power
16 to satisfy the Fourth Amendment”); *Mohamud*, 2014 WL 2866749, at *24-27 (Section 702
17 acquisition and “subsequent querying” of that surveillance collection is reasonable under the
18 Fourth Amendment). All the more so, the promotion of the Government’s national-security
19 interests through Upstream collection justifies the minimal intrusions on Plaintiffs’ Fourth
20 Amendment interests in communications that are not among those the Government retains.¹⁶

21
22 ¹⁵ The conclusions reached by Congress about the value of Section 702 and other FAA
23 intelligence-gathering authorities are echoed in other public reports. *See* PCLOB Report at 2,
24 104, 107, 110 (July 2, 2014) (Section 702 “valuable and effective”; “provides a degree of
25 flexibility not offered by comparable surveillance authorities”; “help[s] the United States learn
26 more about the membership, leadership structure, priorities, tactics, and plans of international
27 terrorist organizations,” leading “to the discovery” and “disruption” of “previously unknown
28 terrorist plots”; and has been “highly valuable” in serving “other foreign intelligence and foreign
policy goals”); The President’s Review Group on Intelligence and Communications
Technologies, *Liberty & Security in a Changing World*, 145 (Dec. 12, 2013) (Exh. D, hereto)
 (“[S]ection 702 has clearly served an important function in helping the United States to uncover
and prevent terrorist attacks both in the United States and around the world.”).

¹⁶ Courts have reached similar conclusions in other national-security contexts, all
involving arguably greater intrusions on Fourth Amendment interests than Plaintiffs have shown.
See also In re Terrorist Bombings of U.S. Embassies in E. Africa, 552 F.3d 157, 172-77 (2d Cir.
2008) (warrantless and broad electronic surveillance of U.S. citizen abroad constitutional

1 At bottom, even if Plaintiffs had presented competent evidence to support the conclusion
 2 that Fourth Amendment seizures and searches occur when Plaintiffs' online communications are
 3 fleetingly copied while transiting the Internet backbone, and then the copies electronically
 4 scanned and destroyed in real time—all without the Government retaining or learning anything
 5 about the communications involved—those searches and seizures fall within the foreign-
 6 intelligence exception to the warrant requirement, and are reasonable under the totality of the
 7 circumstances. Thus no violation of the Fourth Amendment takes place.

8 **D. Even if Plaintiffs Had Presented Evidence of a Seizure or Search, Not**
 9 **Justified Under the Special Needs Doctrine, Their Fourth Amendment**
 10 **Claim Still Could Not Be Litigated Without National-Security Information**
 11 **Protected by the State Secrets Privilege.**

12 Even if the Court were to conclude that Plaintiffs have presented sufficient admissible
 13 evidence of facts, which, if true, would demonstrate that Upstream collection involves a Fourth
 14 Amendment seizure or search of Plaintiffs' communications, and that the minimal intrusion upon
 15 Plaintiffs' possessory and privacy interests is not far outweighed by Upstream collection's
 16 promotion of the Government's compelling interest in national security, then the Government, in
 17 the alternative, would still be entitled to summary judgment on Plaintiffs' Fourth Amendment
 18 claims. That is so, because adjudication of those claims and the Government's defenses thereto
 19 would require disclosure of national-security information subject to the DNI's assertion of the
 20 state secrets privilege.

21 Previously in this litigation the DNI asserted the state secrets privilege over “[a]ny
 22 information concerning NSA intelligence activities, sources, or methods that may relate to or be
 23 necessary to adjudicate plaintiffs’ allegations,” Public Decl. of James R. Clapper, DNI (Sept. 11,
 24 2012) (ECF No. 104) ¶ 10.C; *see* Public Decl. of Frances J. Fleisch, NSA (Sept. 11, 2012) (ECF
 25 No. 105) ¶ 14.B, and renewed that assertion of privilege over “information concerning the scope

26 because the government’s need to “intrude was even greater” than the intrusion); *Cassidy*, 471
 27 F.3d at 70 (searches of carry-on luggage and vehicles before boarding ferries); *MacWade v.*
 28 *Kelly*, 460 F.3d 260, 269-75 (2d Cir. 2006) (random search of subway passengers’ baggage).
 Indeed, given the national-security interests at stake, and the minute extent of any infringement
 on Fourth Amendment interests at alleged Stages 1 and 3, the balance tips even further in the
 Government’s favor than in previous “special needs” cases where the Supreme Court has readily
 upheld, for example, DNA testing, for identification purposes, of persons taken into custody,
King, 133 S. Ct. at 1979-80, and suspicionless urinalysis testing of high-school athletes to
 combat drug abuse. *Earls*, 536 U.S. at 832-34.

1 and operational details of NSA intelligence activities that may [be] relat[ed] to or be necessary to
2 adjudicate plaintiffs' allegations," including "operational details related to the collection of
3 communications under FISA section 702." Public Decl. of James R. Clapper, DNI (Dec. 20,
4 2013) (ECF No. 168) ¶¶ 19.C.1.b, 35 ("Dec. 20, 2013 Clapper Decl."); *see* Public Decl. of
5 Frances J. Fleisch, NSA (Dec. 20, 2013) (ECF No. 169) ¶¶ 35.B.1.b, 38, 39. This Court, in
6 *Jewel*, 965 F. Supp. 2d at 1103, held that "the evidence submitted thus far that the [G]overnment
7 seeks to protect from disclosure contain[s] valid state secrets 'which, in the interest of national
8 security, should not be divulged'" (quoting *United States v. Reynolds*, 345 U.S. 1, 10 (1953)).

9 As explained in the classified supplement submitted *in camera, ex parte*, herewith, the
10 NSA possesses information "concerning operational details related to the collection of
11 communications under FISA section 702," Dec. 20, 2013 Clapper Decl. ¶ 19.C.1.b, that are
12 necessary to a determination of Plaintiffs' seizure and search claims, and the Government's
13 defense thereto. Those facts are set forth in the Classified Decl. of Miriam P., NSA (Sept. 29,
14 2014), also submitted *in camera, ex parte*, herewith; and as confirmed by the DNI, they fall
15 within the scope of his assertion of the state secrets privilege, already made in this case, over the
16 operational details of the Section 702 program. Decl. of James R. Clapper, DNI (Sept. 29, 2014)
17 (Exh. E, hereto) ¶ 2.

18 When, as here, a court has sustained a claim of state secrets privilege, the evidence
19 subject to the privilege is "completely removed from the case," *Kasza*, 133 F.3d at 1166, and the
20 court must then resolve "how the matter should proceed in light of the successful privilege
21 claim." *Al-Haramain Islamic Found. v. Bush*, 507 F.3d 1190, 1202 (9th Cir. 2007) (citation and
22 internal quotation marks omitted): *Jewel*, 965 F. Supp. 2d at 1101. In many situations the
23 exclusion of the privileged evidence will have "no consequences save those resulting from the
24 loss of the evidence," and "the case will proceed accordingly," *Mohamed v. Jeppesen*
25 *Dataplan, Inc.*, 614 F.3d 1070, 1082-83 (9th Cir. 2010) (*en banc*) (quoting *Al-Haramain*, 507
26 F.3d at 1204). In some circumstances, however, "application of the privilege may require
27 dismissal of the action," if, for example, "the privilege deprives the plaintiff of information
28 needed to set forth a prima facie case, or the defendant of information that would otherwise give

1 the defendant a valid defense to the claim” *Id.* at 1083 (quoting *Kasza*, 133 F.3d at 1166);
 2 *Jewel*, 965 F. Supp. 2d at 1100.

3 Here, as explained in the classified *in camera*, *ex parte* supplement submitted herewith, if
 4 the Court were to determine that Plaintiffs have presented competent evidence from which it
 5 could be found that either a seizure or search of Plaintiffs’ communications occurs in the
 6 Upstream collection process, and that the minimal intrusion on Plaintiffs’ Fourth Amendment
 7 interests is not outweighed by the contribution of Upstream collection to national security, then
 8 the operational details presented in the Classified Miriam P. Declaration would be necessary to a
 9 full and fair adjudication of Plaintiffs’ Fourth Amendment claim, including the Government’s
 10 ability to raise and support defenses in addition to those presented herein. That information,
 11 however, is excluded from the case due to the DNI’s valid assertion of the state secrets privilege.
 12 *Kasza*, 133 F.3d at 1166. Accordingly, even barring all other grounds discussed herein on which
 13 Plaintiffs’ motion should be denied, the state secrets doctrine would require that Plaintiffs’
 14 claims be dismissed and judgment awarded instead to the Government. *Jeppesen*, 614 F.3d at
 15 1083; *Kasza*, 133 F.3d at 1166; *Jewel*, 965 F. Supp. 2d at 1100; *see Tenenbaum v. Simonini*, 372
 16 F.3d 776, 777 (6th Cir. 2004).¹⁷

17 CONCLUSION

18 For the foregoing reasons, Plaintiffs’ motion for partial summary judgment on their
 19 Fourth Amendment claim should be denied, and judgment awarded instead to the Government
 20 on Plaintiffs’ Fourth Amendment claim as a matter of law.

21
 22 ¹⁷ The Court’s prior conclusion that the privilege is displaced by 50 U.S.C. § 1806(f),
 23 *Jewel*, 965 F. Supp. 2d at 1105-06, with which the Government respectfully continues to
 24 disagree, does not alter this conclusion. As the Government explained in response to the Court’s
 25 four threshold questions, Plaintiffs must first establish that they are “aggrieved persons” under
 26 § 1806(f) before its procedures can be used to determine the legality of electronic surveillance,
 27 and notwithstanding recent Government disclosures, a § 1806(f) proceeding and an ensuing court
 28 decision risk disclosure of still-classified information that could cause exceptionally grave
 damage to national security. *See Gov. Defs.’ Reply on Threshold Legal Issues* at 4-14 (ECF No.
 185). Moreover, Plaintiffs have expressly declined the use of § 1806(f) proceedings at this time,
 choosing instead to file a motion “based entirely on public evidence” and “defer section 1806(f)
 proceedings.” Plaintiffs’ Responses to the Court’s Four Questions at 7 (ECF No. 177). Lastly,
 the Court held that § 1806(f) displaces the state secrets privilege “with regard to matters within
 FISA’s purview,” *Jewel*, 960 F. Supp. 2d at 1106, but there are no FISA claims against the
 Government left in this case. *See Joint Case Management Statement* at 6-7 (ECF No. 159).

1 Dated: September 29, 2014
2

3 Respectfully Submitted,

4 JOYCE R. BRANDA
Acting Assistant Attorney General

5 JOSEPH H. HUNT
6 Director, Federal Programs Branch

7 ANTHONY J. COPPOLINO
8 Deputy Branch Director
9

10
11 /s/ James J. Gilligan
12 JAMES J. GILLIGAN
Special Litigation Counsel
13 MARCIA BERMAN
Senior Trial Counsel
14 RODNEY PATTON
JULIA BERMAN
Trial Attorneys

15 U.S. Department of Justice
16 Civil Division, Federal Programs Branch
20 Massachusetts Avenue, N.W., Room 6102
17 Washington, D.C. 20001

18 Phone: (202) 514-3358
19 Fax: (202) 616-8470
E-mail: james.gilligan@usdoj.gov

20 *Attorneys for the Government Defendants*
21
22
23
24
25
26
27
28