JOYCE R. BRANDA
Acting Assistant Attorney General

JOSEPH H. HUNT
Director, Federal Programs Branch

ANTHONY J. COPPOLINO
Deputy Branch Director

JAMES J. GILLIGAN
Special Litigation Counsel

MARCIA BERMAN
Senior Trial Counsel

RODNEY PATTON
Trial Attorney

JULIA BERMAN
Trial Attorney

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

Attorneys for the Government Defendants

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

OAKLAND DIVISION

CAROLYN JEWEL, *et al.*, Plaintiffs, v. NATIONAL SECURITY AGENCY, *et al.*, Defendants.	Case No. 4:08-cv-4373-JSW **GOVERNMENT DEFENDANTS' 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

TABLE OF AUTHORITIES

CASES **PAGE(S)**

STATUTES

FEDERAL RULES OF CIVIL PROCEDURE

FEDERAL RULES OF EVIDENCE

LEGISLATIVE MATERIAL

MISCELLANEOUS

INTRODUCTION

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

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

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

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

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

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

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

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

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

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

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

BACKGROUND

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

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

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

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

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

the Attorney General and the DNI may jointly authorize, for up to one year, the "targeting of [non-U.S.] persons reasonably believed to be located outside the United States to acquire foreign intelligence information." 50 U.S.C. § 188la(a), (g).[1] The statute does not define this authority by reference to particular technology, other than to specify that acquisitions of communications under Section 702 must involve "the assistance of an electronic communication service provider." *Id.* § 1881a(g)(2)(A)(vi). Under the express terms of Section 702, the Government may not intentionally target any person known at the time of acquisition to be in the United States or any U.S. person reasonably believed to be located abroad, or intentionally acquire any communication known at the time of acquisition to be wholly domestic. *Id.* § 1881a(b). The acquisition must also be "conducted in a manner consistent with the [F]ourth [A]mendment." *Id.*

B. Operation of the Section 702 Program and Upstream Collection

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

[1] Four requirements must be met for FISC approval of a Section 702 certification. First, the FISC must find that the Government's "targeting procedures" are reasonably designed to ensure that acquisitions conducted under the authorization (a) are limited to targeting non-U.S. persons reasonably believed to be located outside the United States, and (b) will not intentionally 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).

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

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

C. Plaintiff's Motion for Partial Summary Judgment

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

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

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

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

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

[2] To support their assertions regarding activities conducted at the first two stages, 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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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.

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

As the factual foundation for both their standing and the merits of their claims, Plaintiffs rely largely on Klein and Marcus Declarations. These declarations are the principal support for 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.

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

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

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

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

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

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

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

see id. ¶¶ 10, 14, he does not claim to have been present when that alleged clearance was issued, or to have been involved in that work. Instead, an unnamed AT&T employee allegedly told him "to expect a visit from [an] . . . NSA agent," and he received an e-mail from management that "explicitly mentioned the NSA." *Id.* ¶ 10. Such out-of-court statements, offered for the truth of the matters discussed therein, are inadmissible. So too with Mr. Klein's claim that FSS #1 told [Mr. Klein] "the NSA agent" was to interview another unnamed individual ("FSS #2") "for a special job," and FSS #1's claim that "another NSA agent would again visit" in fall 2003 to speak with FSS #3 about "tak[ing] over" FSS #2's "special job." *Id.* ¶ 16.[4]

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

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

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

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

[4] Mr. Klein asserts that NSA agents conducted the interviews discussed above, but fails to 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.

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

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

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

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

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

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

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.

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

[5] Additionally, even if it were based on admissible evidence and the proffered expert testimony were proper under Rule 702, the Marcus Declaration is contrary to the rule that, "[i]n 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).

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

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

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

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

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

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

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

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

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

Plaintiffs continue to assert that their communications are among those "seized" and "searched" in the course of Upstream collection based on the claim that "AT&T allows the [G]overnment to seize the entire communications stream of its customers," including Plaintiffs. Pls.' Mot. at 9-10. Plaintiffs rely entirely on the eight-year-old Klein and Marcus declarations to establish this essential fact. *Id.* at 6 nn. 5-8. But as discussed above, Mr. Klein lacks any personal knowledge of what equipment actually resided or what activities actually occurred in the "SG3 Secure Room" where he claims that copies of all or substantially all of the communications transiting the peering links at AT&T's Folsom Street facility were diverted to the NSA. Mr. Marcus attests to the capabilities of equipment that documents provided by Mr. 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

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

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

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 Issue.

Due to the failings of Plaintiffs' evidence described above, the Court need not consider the impact of the state secrets privilege on the standing issue. However, if the Court were to find Plaintiffs' declarations admissible and sufficiently probative of Plaintiffs' standing to raise a genuine issue meriting further inquiry (which it should not), adjudication f the standing issue could not proceed without risking exceptionally grave damage to national security (a threshold issue on which the Court requested briefing). That is so because operational details of Upstream collection that are subject to the DNI's assertion of the state secrets privilege in this case are necessary to address Plaintiffs' theory of standing. The Government presented this evidence to the Court in the DNI's and NSA's classified declarations of December 20, 2013, and supplements it with the Classified Declaration of Miriam P., NSA, submitted *in camera, ex parte,* herewith. Disclosure of this evidence would risk informing our Nation's adversaries of the operational details of the NSA's Upstream collection, including the identities of electronic-communications-service providers assisting with Upstream collection. The risk of grave damage to national security from disclosure of this evidence remains, notwithstanding the unauthorized public disclosures and official Government releases of previously classified information about 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").

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

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

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

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

IV. PLAINTIFFS SHOULD BE DENIED SUMMARY JUDGMENT, AND JUDGMENT SHOULD INSTEAD BE AWARDED TO THE GOVERNMENT, ON THE MERITS OF PLAINTIFFS' FOURTH AMENDMENT CLAIM.

A. Plaintiffs' Claim of a Seizure at "Stage 1" Fails as a Matter of Fact and Law.

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

Plaintiffs' application for summary judgment on this claim must be denied, and judgment awarded instead to the Government, for two reasons: (1) Plaintiffs have adduced no admissible 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

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

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

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

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

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 law.

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

An evaluation of Plaintiffs' seizure claim must begin with an understanding of what constitutes a seizure for purposes of the Fourth Amendment, a subject bypassed in Plaintiffs' motion. The Fourth Amendment assures the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. amend IV, cl. 1. As the Supreme Court and the Ninth Circuit have explained, "[d]ifferent interests are implicated by a seizure than by a search. A seizure affects only [a] person's possessory interests; a search affects a person's privacy interests." *Segura v. United States*, 468 U.S. 796, 806 (1984) (citations omitted); *United States v. Jacobsen*, 466 U.S. 109, 113 (1984); *Texas v. Brown*, 460 U.S. 730, 747-48 (1983) (Stevens, J., concurring); *United States v. Jefferson*, 566 F.3d 928, 933 (9th Cir. 2009). Accordingly, a Fourth Amendment seizure of property occurs "when there is some meaningful interference with an individual's possessory interests in that property." *Jacobsen*, 466 U.S. at 113; *Jefferson*, 566 F.3d at 933. "'Absent such interference, no fourth amendment seizure will be found.'" *DeBoer v. Pennington*, 206 F.3d 857, 865 (9th Cir. 2000) (quoting *United States v. England*, 971 F.2d 419, 420 (9th Cir. 1992)). *See also, e.g., United States v. Clutter*, 674 F.3d 980, 984-85 (8th Cir. 2012); *United States v. Va Lerie*, 424 F.3d 694, 708 (8th Cir. 2005) (no seizure where temporary removal of bus passenger's checked luggage 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,

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

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

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

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

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

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

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

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

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

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

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

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

[6] The fact that the data actually retained by the Government are "not at issue here," Pls.' Mot. at 9, also eliminates any valid basis for comparing Stage 1 of the alleged surveillance process here to the NSA's Cold War-era "Operation Shamrock," or for Plaintiffs' continued reliance on this Court's prior decision in *Hepting v. AT&T*, 439 F. Supp. 2d 974 (N.D. Cal. 2006), *id.* at 16-17, 18. *See* Intelligence Activities: Hrgs. Before the Sen. Select Comm. To Study Governmental Operations With Respect to Intelligence Activities, 94th Cong., Vol. V, 57-59 (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).

[7] Plaintiffs confuse the issue when they assert, in support of their seizure claim, that they have a reasonable expectation of privacy in the copied communications. Pls.' Mot. at 17. By definition, the violation of an individual's reasonable expectation of privacy constitutes a search, 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.

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

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

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

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

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

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

Id. at 707 (emphasis added).

The Court extended the logic of *Place* to a chemical test for narcotics in *Jacobsen*. In 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"—

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

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

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

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

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.

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

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 information.

Plaintiffs argue that the alleged Stage 1 copying and Stage 3 scanning of their communications violate the Fourth Amendment because "[n]ational security does not excuse the need for a warrant" to conduct these activities. Pls.' Mot. at 14. But under the Supreme 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)

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

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

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

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

[8] Under the "special needs" doctrine, the Supreme Court has permitted warrantless stops 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.

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

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

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

[9] Plaintiffs' reliance (Pls.' Mot. at 13, 15-17, 23, 25) on *Keith* and *Berger v. New York*, 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.

of mass destruction, and clandestine intelligence activities of foreign intelligence services. *See id.* § 1801(e); *see also In re Directives*, 551 F.3d at 1011 (PAA, the predecessor to the FAA, had the "stated purpose" of "garnering foreign intelligence" and "[t]here [was] no indication that the collections of information [were] primarily related to ordinary criminal-law enforcement purposes"). *Cf. In re Sealed Case*, 310 F.3d at 745-46 ("programmatic purpose" of obtaining foreign intelligence was "a special need"); *Cassidy v. Chertoff*, 471 F.3d 67, 82 (2d Cir. 2006) (interest in preventing terrorist attacks goes "well beyond" law enforcement). Plaintiffs make no serious argument that Upstream collection is undertaken for routine law enforcement or any purpose other than furthering "legitimate national security concerns." Pls.' Mot. at 25.[10]

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

[10] Plaintiffs do quarrel, however, that collection under Section 702 does not meet the requirements of the special-needs exception because first, the category of foreign intelligence includes "information that relates to national defense" and "foreign affairs," and second, because obtaining foreign intelligence need only be a "significant purpose" of an acquisition rather than 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.

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

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

Accordingly, the alleged seizure and search about which Plaintiffs complain fall under the Fourth Amendment's "special needs" exception to the warrant requirement.

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.

Even where a warrant and probable cause are not required, searches and seizures remain subject to the Fourth Amendment's "traditional standards of reasonableness." *Maryland v. King*, 133 S. Ct. 1958, 1970 (2013). In assessing the reasonableness of the putative "seizure" and "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).

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

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

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

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

cf. King, 133 S. Ct. at 1979-80 (statutory protections guarding against further invasion of privacy contribute to reasonableness). The statute requires the DNI and the Attorney General to certify, and the FISC to approve, that a significant purpose of an acquisition is to obtain foreign intelligence information, *id.* § 1881a (g)(2)(A)(v), (i). Section 702 also requires the DNI and the Attorney General annually to certify—and the FISC to so find—that acquisitions will comply with the Fourth Amendment and the statutorily required targeting procedures are reasonably designed to target only non-U.S. persons reasonably believed to be located outside the United States, that is, those who do not have Fourth Amendment rights, *United States v. Verdugo-Urquidez*, 494 U.S. 259, 271 (1990). *See* 50 U.S.C. § 1881a(a), (b), (d)(2), (g), (i).[12] Along with the Executive's reports to the FISC and to Congress about "compliance with the targeting . . . procedures," *id.* § 1881a(l)(1), these requirements contribute to the reasonableness of the collection under Section 702. *See Mohamud*, 2014 WL 2866749, at *27.[13]

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

[12] Plaintiffs are wrong to complain that the "Executive alone makes all [the] decisions" about targeting "without judicial oversight," Pls.' Mot. at 23, because the statute imposes significant limitations on permissible targeting and the purposes for which information may be collected, 50 U.S.C. § 1881a(b), (g)(2)(A)(v), and compliance with those limitations is reviewed by the FISC. *See id.* § 1881a(i); PCLOB Report at 26-28 (describing FISC's role as "extensive" in some respects). They are also wrong in dismissing the FISC's role in the process as that of "an administrative agency" instead of an Article III court. Pls.' Mot. at 21-22. The FISC 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).

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

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

> importance of the collection of foreign intelligence under the [FAA] . . . cannot be underscored enough. In short, intelligence collected under the FAA is critically important to maintaining our national security. The information collected under 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.

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

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

[14] Indeed, even those members of the House Judiciary Committee who "strongly oppose[d]" reauthorization, H.R. Rep. No. 112-645(I), 112th Cong., 2d Sess., at 13 (Aug. 2, 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).

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

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

---

[15] The conclusions reached by Congress about the value of Section 702 and other FAA intelligence-gathering authorities are echoed in other public reports. *See* PCLOB Report at 2, 104, 107, 110 (July 2, 2014) (Section 702 "valuable and effective"; "provides a degree of flexibility not offered by comparable surveillance authorities"; "help[s] the United States learn more about the membership, leadership structure, priorities, tactics, and plans of international terrorist organizations," leading "to the discovery" and "disruption" of "previously unknown 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

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

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.

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

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

---

because the government's need to "intrude was even greater" than the intrusion); *Cassidy*, 471 F.3d at 70 (searches of carry-on luggage and vehicles before boarding ferries); *MacWade v. 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.

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

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

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

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

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

CONCLUSION

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

[17] The Court's prior conclusion that the privilege is displaced by 50 U.S.C. § 1806(f), *Jewel*, 965 F. Supp. 2d at 1105-06, with which the Government respectfully continues to disagree, does not alter this conclusion. As the Government explained in response to the Court's four threshold questions, Plaintiffs must first establish that they are "aggrieved persons" under § 1806(f) before its procedures can be used to determine the legality of electronic surveillance, and notwithstanding recent Government disclosures, a § 1806(f) proceeding and an ensuing court 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).

Dated: September 29, 2014

Respectfully Submitted,

JOYCE R. BRANDA
Acting Assistant Attorney General

JOSEPH H. HUNT
Director, Federal Programs Branch

ANTHONY J. COPPOLINO
Deputy Branch Director

/s/ James J. Gilligan
JAMES J. GILLIGAN
Special Litigation Counsel
MARCIA BERMAN
Senior Trial Counsel
RODNEY PATTON
JULIA BERMAN
Trial Attorneys

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

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

Attorneys for the Government Defendants

EXHIBIT A

NSA Director of Civil Liberties and Privacy Office Report

NSA's Implementation of Foreign Intelligence Surveillance Act Section 702

April 16, 2014

National Security Agency, Civil Liberties and Privacy Office
Report
NSA's Implementation of Foreign Intelligence Surveillance Act Section 702

April 16, 2014

INTRODUCTION

This report was prepared by the National Security Agency (NSA) Civil Liberties and Privacy Office as part of its responsibilities to enhance communications and transparency with the public and stakeholders. Its Director is the primary advisor to the Director of NSA when it comes to matters of civil liberties and privacy. Created in January 2014, the Office is also charged with ensuring that civil liberties and privacy protection are integrated into NSA activities. The intent of this paper is to help build a common understanding that can serve as a foundation for future discussions about the existing civil liberties and privacy protections.

The mission of NSA is to make the nation safer by providing policy makers and military commanders with timely foreign intelligence and by protecting national security information networks. NSA collects foreign intelligence based on requirements from the President, his national security team, and their staffs through the National Intelligence Priorities Framework. NSA fulfills these national foreign intelligence requirements through the collection, processing, and analysis of communications or other data, passed or accessible by radio, wire or other electronic means.

NSA's authority to conduct signals intelligence collection for foreign intelligence and counterintelligence purposes is provided primarily by Section 1.7(c)(1) of Executive Order 12333, as amended. The execution of NSA's signals intelligence mission must be conducted in conformity with the Fourth Amendment. This includes NSA's acquisition of communications to which a U.S. person is a party under circumstances in which the U.S. person has a reasonable expectation of privacy. The Foreign Intelligence Surveillance Act of 1978 (FISA) further regulates certain types of foreign intelligence collection, including that which occurs with compelled assistance from U.S. communications providers.

This Report describes one way in which NSA meets these responsibilities while using Section 702 of FISA, as amended by the FISA Amendments Act of 2008. Although multiple federal agencies participate in Section 702 collection, this paper describes the process by which NSA obtains, uses, shares, and retains communications of foreign intelligence value pursuant to Section 702. It also describes existing privacy and civil liberties protections built into the process.

The NSA Civil Liberties and Privacy Office (CLPO) used the Fair Information Practice Principles (FIPP)[1] as an initial tool to describe the existing civil liberties and privacy protections in place for collection done under Section 702 authority.[2]

SECTION 702 OF FISA

Section 702 of FISA was widely and publicly debated in Congress both during the initial passage in 2008 and the subsequent re-authorization in 2012. It provides a statutory basis for NSA, with the compelled assistance of electronic communication service providers, to target non-U.S. persons reasonably believed to be located outside the U.S. in order to acquire foreign intelligence information. Given that Section 702 only allows for the targeting of non-U.S. persons outside the U.S., it differs from most other sections of FISA. It does not require an individual determination by the U.S. Foreign Intelligence Surveillance Court (FISC) that there is probable cause to believe the target is a foreign power or an agent of a foreign power. Instead, the FISC reviews annual topical certifications executed by the Attorney General (AG) and the Director of National Intelligence (DNI) to determine if these certifications meet the statutory requirements. The FISC also determines whether the statutorily required targeting and minimization procedures used in connection with the certifications are consistent with the statute and the Fourth Amendment. The targeting procedures are designed to ensure that Section 702 is only used to target non-U.S. persons reasonably believed to be located outside the U.S.

The minimization procedures are designed to minimize the impact on the privacy on U.S. persons by minimizing the acquisition, retention, and dissemination of non-publicly available U.S. person information that was lawfully, but incidentally acquired under Section 702 by the targeting of non-U.S. persons reasonably believed to be located outside the U.S. Under these certifications the AG and the DNI issue directives to electronic communication service providers (service providers) that require these service providers to "immediately provide the Government with all information … or assistance necessary to accomplish the acquisition [of foreign intelligence information] in a manner that will protect the secrecy of the acquisition…." The Government's acquisition of communications under its Section 702 authority thus takes place pursuant to judicial review and with the knowledge of the service providers.

NSA cannot intentionally use Section 702 authority to target any U.S. citizen, any other U.S. person, or anyone known at the time of acquisition to be located within the U.S. The statute also prohibits the use of Section 702 to intentionally acquire any communication as to which the

[1] The FIPPS are the recognized principles for assessing privacy impacts. They have been incorporated into EO13636, *Improving Critical Infrastructure Cybersecurity* and the National Strategy for Trusted Identities in Cyberspace. These principles are rooted in the U.S. Department of Health, Education and Welfare's seminal 1973 report, "Records, Computers and the Rights of Citizens." The FIPPs have been implemented in the Privacy Act of 1974, with certain exemptions, including ones that apply to certain national security and law enforcement activities.

[2] NSA CLPO will continue to refine its assessment tools to best suit the mission of NSA, as a member of the Intelligence Community, and to protect civil liberties and privacy.

sender and all intended recipients are known at the time of acquisition to be located inside the U.S. Similarly, the statute prohibits the use of Section 702 to conduct "reverse targeting" (i.e., NSA may not intentionally target a person reasonably believed to be located outside of the U.S. if the purpose of such acquisition is to target a person reasonably believed to be located inside the U.S.). All acquisitions conducted pursuant to Section 702 must be conducted in a manner consistent with the Fourth Amendment. NSA's FISC-approved targeting procedures permit NSA to target a non-U.S. person reasonably believed to be located outside the U.S. if the intended target possesses, is expected to receive, and/or is likely to communicate foreign intelligence information concerning one of the certifications executed by the AG and DNI. Although the purpose of Section 702 is to authorize targeting of non-U.S. persons outside the U.S., the statute's requirement for minimization procedures recognizes that such targeted individuals or entities may communicate about U.S. persons or with U.S. persons. For this reason, NSA also must follow FISC-approved minimization procedures that govern the handling of any such communications.

NSA must report to the Office of the Director of National Intelligence (ODNI) and the Department of Justice (DOJ) any and all instances where it has failed to comply with the targeting and/or minimization procedures. In addition, ODNI and DOJ have access to documentation concerning each of NSA's Section 702 targeting decisions and conduct regular reviews in order to provide independent oversight of NSA's use of the authority. The FISC Rules of Procedure require the Government to notify the Court of all incidents of non-compliance with applicable law or with an authorization granted by the Court. The Government reports Section 702 compliance incidents to the Court via individual notices and quarterly reports. In addition, the Government reports all Section 702 compliance incidents to Congress in the Attorney General's Semiannual Report. Depending on the type or severity of compliance incident, NSA may also promptly notify the Congressional Intelligence Committees, as well as the President's Intelligence Oversight Board of an individual compliance matter.

Existing Privacy and Civil Liberties Protections: Each of the three branches of federal government oversees NSA's use of the Section 702 authorities. NSA provides transparency to its oversight bodies (Congress, DOJ, ODNI, DoD, the President's Intelligence Oversight Board and the FISC) through regular briefings, court filings, and incident reporting. In addition, DOJ and ODNI conduct periodic reviews of NSA's use of the authority and report on those reviews. More recently, at the direction of the President, the Government has provided additional transparency to the public regarding the program by declassifying FISC opinions and related documents. Although FISA surveillance is normally kept secret from the targets of the surveillance, there are exceptions. For example, if the Government intends to use the results of FISA surveillance, to include Section 702 surveillance, in a trial or other proceeding against a person whose communications were collected, the Government must notify the person so the person can challenge whether the communications were acquired lawfully. These protections implement the general Fair Information Practice Principle (FIPP) of transparency.

HOW NSA IMPLEMENTS SECTION 702 of FISA

TRAINING

Before an analyst gains access to any NSA signals intelligence data, the analyst must complete specialized training on the legal and policy guidelines that govern the handling and use of the data. Additional training is required for access to Section 702 data. These annual mandatory training requirements include scenario-based training, required reading, and a final competency test. The analyst must pass this test before being granted access. Furthermore, if a compliance incident involves a mistake or misunderstanding of relevant policies, the analyst is re-trained in order to continue to have access to the data acquired pursuant to Section 702.

IDENTIFYING AND TASKING A SELECTOR

Next in the Section 702 process is for an NSA analyst to identify a non-U.S. person located outside the U.S. who has and/or is likely to communicate foreign intelligence information as designated in a certification. For example, such a person might be an individual who belongs to a foreign terrorist organization or facilitates the activities of that organization's members. Non-U.S. persons are not targeted unless NSA has reason to believe that they have and/or are likely to communicate foreign intelligence information as designated in a certification; U.S. persons are never targeted.

Once the NSA analyst has identified a person of foreign intelligence interest who is an appropriate target under one of the FISC-approved Section 702 certifications, that person is considered the target. The NSA analyst attempts to determine how, when, with whom, and where the target communicates. Then the analyst identifies specific communications modes used by the target and obtains a unique identifier associated with the target – for example, a telephone number or an email address. This unique identifier is referred to as a selector. The selector is not a "keyword" or particular term (e.g., "nuclear" or "bomb"), but must be a specific communications identifier (e.g., e-mail address).

Next the NSA analyst must verify that there is a connection between the target and the selector and that the target is reasonably believed to be (a) a non-U.S. person and (b) located outside the U.S. This is not a 51% to 49% "foreignness" test. Rather the NSA analyst will check multiple sources and make a decision based on the totality of the information available. If the analyst discovers any information indicating the targeted person may be located in the U.S. or that the target may be a U.S. person, such information must be considered. In other words, if there is conflicting information about the location of the person or the status of the person as a non-U.S. person, that conflict must be resolved before targeting can occur.

For each selector, the NSA analyst must document the following information: (1) the foreign intelligence information expected to be acquired, as authorized by a certification, (2) the information that would lead a reasonable person to conclude the selector is associated with a

non-U.S. person, and (3) the information that would similarly lead a reasonable person to conclude that this non-U.S. person is located outside the U.S. This documentation must be reviewed and approved or denied by two senior NSA analysts who have satisfied additional training requirements. The senior NSA analysts may ask for more documentation or clarification, but regardless must verify that all requirements have been met in full. NSA tracks the submission, review, and approval process through the documentation and the senior NSA analysts' determinations are retained for further review by NSA's compliance elements, as well as external oversight reviewers from DOJ and ODNI. Upon approval, the selector may be used as the basis for compelling a service provider to forward communications associated with the given selector. This is generally referred to as "tasking" the selector.

Existing Privacy and Civil Liberties Protections: NSA trains its analysts extensively through a variety of means to ensure that analysts fully understand their responsibilities and the specific scope of this authority. If the analyst fails to meet the training standards, the analyst will not have the ability to use the Section 702 authority for collection purposes. If the analyst fails to maintain ongoing training standards, the analyst will lose the ability to use the Section 702 authority for collection purposes and all ability to retrieve any data previously collected under the authority. NSA requires any authorized and trained analyst seeking to task a selector using Section 702 to document the three requirements for use of the authority – that the target is connected sufficiently to the selector for an approved foreign intelligence purpose, that the target is a non-U.S. person, and that the target is reasonably believed to be located outside the U.S. This documentation must be reviewed, validated, and approved by the senior analysts who have received additional training. These protections implement the general FIPPs of purpose specification, accountability and auditing, and minimization.

ACCESSING AND ASSESSING COMMUNICATIONS OBTAINED UNDER SECTION 702 AUTHORITY

Once senior analysts have approved a selector as compliant, the service providers are legally compelled to assist the government by providing the relevant communications. Therefore, tasking under this authority takes place with the knowledge of the service providers. NSA receives information concerning a tasked selector through two different methods.

In the first, the Government provides selectors to service providers through the FBI. The service providers are compelled to provide NSA with communications to or from these selectors. This has been generally referred to as the PRISM program.

In the second, service providers are compelled to assist NSA in the lawful interception of electronic communications to, from, or about tasked selectors. This type of compelled service provider assistance has generally been referred to as Upstream collection. NSA's FISC-approved targeting procedures include additional requirements for such collection designed to prevent acquisitions of wholly domestic communications. For example, in certain circumstances NSA's procedures require that it employ an Internet Protocol filter to ensure that the target is

located overseas. The process for approving the selectors for tasking is the same for both PRISM and Upstream collection.

Once NSA has received communications of the tasked selector, NSA must follow additional FISC-approved procedures known as the minimization procedures. These procedures require NSA analysts to review at least a sample of communications acquired from all selectors tasked under Section 702, which occurs on a regular basis to verify that the reasonable belief determination used for tasking remains valid.

The NSA analyst must review a sample of communications received from the selectors to ensure that they are in fact associated with the foreign intelligence target and that the targeted individual or entity is not a U.S. person and is not currently located in the U.S. If the NSA analyst discovers that NSA is receiving communications that are not in fact associated with the intended target or that the user of a tasked selector is determined to be a U.S. person or is located in the U.S., the selector must be promptly "detasked." As a general rule, in the event that the target is a U.S. person or in the U.S., all other selectors associated with the target also must be detasked.

Existing Privacy and Civil Liberties Protections: In addition to extensive training, the analyst is required to review the collection to determine that it is associated with the targeted selector and is providing the expected foreign intelligence shortly after the tasking starts and at least annually thereafter. This review allows NSA to identify possible problems with the collection and provides an additional layer of accountability. In addition, NSA has technical measures that alert the NSA analysts if it appears a selector is being used from the U.S. These protections implement the general FIPPs of purpose specification, minimization, accountability and auditing, data quality, and security.

NSA PROCESSING AND ANALYSIS OF COMMUNICATIONS OBTAINED UNDER SECTION 702 AUTHORITY

Communications provided to NSA under Section 702 are processed and retained in multiple NSA systems and data repositories. One data repository, for example, might hold the contents of communications such as the texts of emails and recordings of conversations, while another, may only include metadata, i.e., basic information about the communication, such as the time and duration of a telephone call, or sending and receiving email addresses.

NSA analysts may access communications obtained under Section 702 authority for the purpose of identifying and reporting foreign intelligence. They access the information via "queries," which may be date-bound, and may include alphanumeric strings such as telephone numbers, email addresses, or terms that can be used individually or in combination with one another. FISC-approved minimization procedures govern any queries done on Section 702-derived information. NSA analysts with access to Section 702-derived information are trained in the proper construction of a query so that the query is reasonably likely to return valid foreign

intelligence and minimizes the likelihood of returning non-pertinent U.S. person information. Access by NSA analysts to each repository is controlled, monitored, and audited. There are, for example, automated checks to determine if an analyst has completed all required training prior to returning information responsive to a query. Further, periodic spot checks on queries by NSA analysts are conducted.

Since October 2011 and consistent with other agencies' Section 702 minimization procedures, NSA's Section 702 minimization procedures have permitted NSA personnel to use U.S. person identifiers to query Section 702 collection when such a query is reasonably likely to return foreign intelligence information. NSA distinguishes between queries of communications content and communications metadata. NSA analysts must provide justification and receive additional approval before a content query using a U.S. person identifier can occur. To date, NSA analysts have queried Section 702 content with U.S. person identifiers less frequently than Section 702 metadata. For example, NSA may seek to query a U.S. person identifier when there is an imminent threat to life, such as a hostage situation. NSA is required to maintain records of U.S. person queries and the records are available for review by both DOJ and ODNI as part of the external oversight process for this authority. Additionally, NSA's procedures prohibit NSA from querying Upstream data with U.S. person identifiers.

Existing Privacy and Civil Liberties Protections: In addition to the training and access controls, NSA maintains audit trails for all queries of the Section 702 data. NSA's Signals Intelligence Directorate's compliance staff routinely reviews a portion of all queries that include U.S. person identifiers to ensure that all such queries are only conducted when appropriate. Personnel from DOJ and ODNI provide an additional layer of oversight to ensure that NSA is querying the data appropriately. These protections implement the general FIPPs of security, accountability and auditing, and data quality.

NSA DISSEMINATION OF INTELLIGENCE DERIVED FROM COMMUNICATIONS OBTAINED UNDER SECTION 702 AUTHORITY

NSA only generates signals intelligence reports when the information meets a specific intelligence requirement, regardless of whether the proposed report contains U.S. person information. Dissemination of information about U.S. persons in any NSA foreign intelligence report is expressly prohibited unless that information is necessary to understand foreign intelligence information or assess its importance, contains evidence of a crime, or indicates a threat of death or serious bodily injury. Even if one or more of these conditions apply, NSA may include no more than the minimum amount of U.S. person information necessary to understand the foreign intelligence or to describe the crime or threat. For example, NSA typically "masks" the true identities of U.S. persons through use of such phrases as "a U.S. person" and the suppression of details that could lead to him or her being successfully identified by the context. Recipients of NSA reporting can request that NSA provide the true identity of a masked U.S. person referenced in an intelligence report if the recipient has a legitimate need to know the identity. Under NSA policy, NSA is allowed to unmask the identity only under certain

conditions and where specific additional controls are in place to preclude its further dissemination, and additional approval has been provided by one of seven designated positions at NSA. Additionally, together DOJ and ODNI review the vast majority of disseminations of information about U.S. persons obtained pursuant to Section 702 as part of their oversight process.

Existing Privacy and Civil Liberties Protections: As noted above, NSA only generates signals intelligence reports when the information meets a specific intelligence requirement, regardless of whether the proposed report contains U.S. person information or not. Additionally, NSA's Section 702 minimization procedures require any U.S. person information to be minimized prior to dissemination, thereby reducing the impact on privacy for U.S. persons. The information may only be unmasked in specific instances consistent with the minimization procedures and NSA policy. These protections implement the general FIPPs of minimization and purpose specification.

RETENTION OF UNEVALUATED COMMUNICATIONS OBTAINED UNDER SECTION 702 AUTHORITY

The maximum time that specific communications' content or metadata may be retained by NSA is established in the FISC-approved minimization procedures. The unevaluated content and metadata for PRISM or telephony data collected under Section 702 is retained for no more than five years. Upstream data collected from Internet activity is retained for no more than two years. NSA complies with these retention limits through an automated process.

NSA's procedures also specify several instances in which NSA must destroy U.S. person collection promptly upon recognition. In general, these include any instance where NSA analysts recognize that such collection is clearly not relevant to the authorized purpose of the acquisition nor includes evidence of a crime. Additionally, absent limited exceptions, NSA must destroy any communications acquired when any user of a tasked account is found to have been located in the U.S. at the time of acquisition.

Existing Privacy and Civil Liberties Protections: NSA has policies, technical controls, and staff in place to ensure the data is retained in accordance with the FISC-approved procedures. The automated process to delete the collection at the end of the retention period applies to both U.S. person and non U.S. person the information. There is an additional manual process for the destroying information related to U.S. Persons where NSA analysts have recognized the collection is clearly not relevant to the authorized purpose of the acquisition nor includes evidence of a crime. These protections implement the general FIPPs of minimization and security.

ORGANIZATIONAL MANAGEMENT, COMPLIANCE, AND OVERSIGHT

NSA is subject to rigorous internal compliance and external oversight. Like many other regulated entities, NSA has an enterprise-wide compliance program, led by NSA's Director of Compliance, a position required by statute. NSA's compliance program is designed to provide precision in NSA's activities to ensure that they are consistently conducted in accordance with law and procedure, including in this case the Section 702 certifications and accompanying Section 702 targeting and minimization procedures and additional FISC requirements. As part of the enterprise-wide compliance structure, NSA has compliance elements throughout its various organizations. NSA also seeks to detect incidents of non-compliance at the earliest point possible. When issues of non-compliance arise regarding the way in which NSA carries out the FISC-approved collection, NSA takes corrective action and, in parallel, NSA must report incidents of non-compliance to ODNI and DOJ for further reporting to the FISC and Congress, as appropriate or required.

These organizations, along with the NSA General Counsel, the NSA Inspector General, and most recently the Director of Civil Liberties and Privacy have critical roles in ensuring all NSA operations proceed in accordance with the laws, policies, and procedures governing intelligence activities. Additionally, each individual NSA analyst has a responsibility for ensuring that his or her personal activities are similarly compliant. Specifically, this responsibility includes recognizing and reporting all situations in which he or she may have exceeded his or her authority to obtain, analyze, or report intelligence information under Section 702 authority.

Compliance: NSA reports all incidents in which, for example, it has or may have inappropriately queried the Section 702 data, or in which an analyst may have made typographical errors or dissemination errors. NSA personnel are obligated to report when they believe NSA is not, or may not be, acting consistently with law, policy, or procedure. If NSA is not acting in accordance with law, policy, or procedure, NSA will report through its internal and external intelligence oversight channels, conduct reviews to understand the root cause, and make appropriate adjustments to its procedures.

If NSA discovers that it has tasked a selector that is used by a person in the U.S. or by a U.S. person, then NSA must cease collection immediately and, in most cases must also delete the relevant collected data and cancel or revise any disseminated reporting based on this data. NSA encourages self-reporting by its personnel and seeks to remedy any errors with additional training or other measures as necessary. Following an incident, a range of remedies may occur: admonishment, written explanation of the offense, request to acknowledge a training point that the analyst might have missed during training, and/or required retesting. In addition to reporting described above, any intentional violation of law would be referred to the NSA Office of Inspector General. To date there have been no such instances, as most recently confirmed by the President's Review Group on Intelligence and Communications Technology.

External Oversight: As required by the Section 702 targeting procedures, both DOJ and ODNI conduct routine oversight reviews. Representatives from both agencies visit NSA on a bi-monthly basis. They examine all tasking datasheets that NSA provides to DOJ and ODNI to determine whether the tasking sheets meet the documentation standards required by NSA's targeting procedures and provide sufficient information for the reviewers to ascertain the basis for NSA's foreignness determinations. For those records that satisfy the standards, no additional documentation is requested. For those records that warrant further review, NSA provides additional information to DOJ and ODNI during or following the onsite review. NSA receives feedback from the DOJ and ODNI team and incorporates this information into formal and informal training to analysts. DOJ and ODNI also review the vast majority of disseminated reporting that includes U.S. person information.

Existing Privacy and Civil Liberties Protections: The compliance and oversight processes allow NSA to identify any concerns or problems early in the process so as to minimize the impact on privacy and civil liberties. These protections implement the general FIPPs of transparency to oversight organizations and accountability and auditing.

CONCLUSION

This Report, prepared by NSA's Office of Civil Liberties and Privacy, provides a comprehensive description of NSA's Section 702 activities. The report also documents current privacy and civil liberties protections.

EXHIBIT B

(U) The Intelligence Community's Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act

(U) THE INFORMATION CONTAINED IN THIS REPORT DESCRIBES SOME OF THE MOST SENSITIVE FOREIGN INTELLIGENCE COLLECTION PROGRAMS CONDUCTED BY THE UNITED STATES GOVERNMENT. THIS INFORMATION IS HIGHLY CLASSIFIED. PUBLICLY DISCLOSING ANY OF THIS INFORMATION WOULD BE EXPECTED TO CAUSE EXCEPTIONALLY GRAVE DAMAGE TO OUR NATION'S INTELLIGENCE CAPABILITIES AND TO NATIONAL SECURITY. THEREFORE IT IS IMPERATIVE THAT THOSE WHO ACCESS THIS DOCUMENT ABIDE BY THEIR OBLIGATION NOT TO DISCLOSE THIS INFORMATION TO ANY PERSON UNAUTHORIZED TO RECEIVE IT.

(U) Introduction

~~(S//NF)~~ Section 702 of the Foreign Intelligence Surveillance Act (FISA), added by the FISA Amendments Act (FAA) of 2008, has proven to be a critical tool in the Government's efforts to acquire foreign intelligence necessary to protect the Nation's security, while at the same time establishing rigorous safeguards to protect the privacy interests of U.S. persons. The FAA has significantly enhanced the capability of the Intelligence Community to collect information about [redacted]. Section 702, along with other important provisions of the FAA, will expire at the end of this year unless reauthorized by Congress. Reauthorization is the top legislative priority of the Intelligence Community. This paper provides an overview of all of the expiring provisions of the FAA, including section 704, which provides greater protection for collection activities directed against U.S. persons overseas than existed before passage of the FAA. The principal focus of the paper is section 702, including the extensive oversight of its use and the importance of this authority to our national security. An attachment contains examples of the valuable intelligence section 702 collection has provided.

(U) I. Overview of Section 702

(U) Legal Requirements

~~(S//NF)~~ Many terrorists and other foreign intelligence targets abroad use communications services based in this country, [redacted]

Classified By: 2381928
Declassify On: 20320108
Derived From: NSA/CSSM 1-52

[redacted] These provisions require a finding of probable cause that the overseas target is a foreign power or an agent of a foreign power, such as an international terrorist organization, and that the target is using or about to use the targeted facility, such as a telephone number or e-mail account. The Attorney General, and subsequently the Foreign Intelligence Surveillance Court (FISC), must approve each application. In effect, the Intelligence Community had to treat the overseas foreign target the same way as a U.S. person or person in the United States and obtain an individual order, based on a finding of probable cause by a neutral magistrate, even though the target was neither a U.S. person nor a person in the United States. Non-U.S. persons outside the United States generally are not entitled to the protections of the Fourth Amendment. Accordingly, the Constitution does not require this burdensome practice.

(S//NF) Section 702 remedies these shortcomings and permits the Government to acquire, safely and efficiently from providers in the United States, communications where non-U.S. persons located abroad are targeted for the purpose of acquiring foreign intelligence information. At the same time, it provides a comprehensive regime of oversight by all three branches of Government to protect the constitutional and privacy interests of Americans.

(U//FOUO) Under section 702, instead of issuing individual orders, the FISC, which is comprised of federal judges from around the country appointed by the Chief Justice of the Supreme Court, approves annual certifications submitted by the Attorney General and the Director of National Intelligence (DNI) that identify broad categories of foreign intelligence which may be collected. The statute stipulates several criteria for collection. First, the Attorney General and the DNI must certify that a significant purpose of an acquisition is to obtain foreign intelligence information. Second, an acquisition may intentionally target only non-U.S. persons. Third, an acquisition may not intentionally target any person known at the time of the acquisition to be in the United States. Fourth, an acquisition may not target a person outside the United States for the purpose of targeting a particular, known person in this country. Fifth, section 702 protects domestic communications by prohibiting the intentional acquisition of "any communication as to which the sender and all intended recipients are known at the time of the acquisition" to be in the United States. Finally, any acquisition must be consistent with the Fourth Amendment. The certifications are the legal basis for targeting specific individuals overseas and, based on the certifications, the Attorney General and the DNI can direct communications providers in this country to assist the Government in acquiring these targets' communications.

(U) Because when originally passed Congress understood that U.S.-person communications would incidentally be acquired when targeting foreign communications, to ensure compliance with these provisions, section 702 requires the Attorney General, in consultation with the DNI, to adopt targeting and minimization procedures. Under the statute, the targeting procedures must be reasonably designed to ensure that an acquisition is limited to targeting persons reasonably believed to be located outside the United States, and to prevent the intentional acquisition of purely domestic communications. The minimization procedures govern how the Intelligence Community treats the identities of any U.S. persons whose communications might be incidentally intercepted and regulate the handling of any nonpublic information concerning U.S.

persons that is acquired. These minimization procedures must meet the same standard as the minimization procedures required by other provisions of FISA. The FISC reviews the targeting and minimization procedures for compliance with the requirements of both the statute and the Fourth Amendment, and the appropriate congressional committees receive copies of them. By approving the certifications submitted by the Attorney General and the DNI as well as the targeting and minimization procedures, the FISC plays a vital role in ensuring that acquisitions under section 702 are conducted in a lawful and appropriate manner.

(U) **Implementation**

~~(S//NF)~~ Currently, the Attorney General and the DNI have authorized the acquisition of foreign intelligence information under section 702 [redacted] The Attorney General and the DNI must resubmit these certifications to the FISC for review and renewal at least once a year. Using these certifications, Intelligence Community elements participate in the tasking of selectors for telephony, as well as electronic communications accounts, such as e-mail addresses.

~~(S//NF)~~ NSA takes the lead in targeting and tasks both telephone and electronic communications selectors to acquire communications [redacted]. NSA's targeting procedures require that there be an appropriate foreign intelligence purpose for the acquisition and that the selector be used by a non-U.S. person reasonably believed to be located outside the United States. To determine the location of a user, an analyst must, as appropriate, examine the lead information about the potential target or selector; [redacted]

~~(S//NF)~~ [redacted]. Because NSA has already made a "foreignness" determination for these selectors in accordance with its FISC-approved targeting procedures, FBI's targeting role differs from that of NSA. FBI is not required to second-guess NSA's targeting determinations. It must, however, review and understand NSA's targeting determinations, [redacted].

~~(TS//SI//NF)~~ Once a target has been approved, NSA uses two means to acquire [redacted] electronic communications. First, [redacted], it acquires such communications directly from U.S.-based ISPs. This is known as PRISM collection. Using PRISM, NSA currently collects against approximately [redacted] selectors at any given time.

~~(TS//SI//NF)~~ Second, in addition to collection directly from ISPs, NSA collects telephone and electronic communications as they transit the Internet "backbone" within the United States. This

is known as "upstream" collection [redacted], the volume of communications acquired upstream is much smaller than that obtained through PRISM. In June 2011, for example, it made up only about 11% of the overall section 702 volume. [redacted]

~~(TS//SI//NF)~~ Upstream collection enables NSA to target terrorists [redacted] It also lets NSA collect electronic communications that contain the targeted e-mail address in the body of a communication between two third parties. Finally, NSA obtains certain international or foreign telephone communications from this collection.

~~(TS//SI//NF)~~ Once acquired, all communications are routed to NSA. NSA also can designate the communications from specified selectors acquired through PRISM collection to be "dual-routed" to other Intelligence Community elements. Each agency that receives the collection has its own minimization procedures that have been approved by the FISC and may retain and disseminate communications acquired under section 702 only in accordance with those procedures. In general, before an agency may disseminate information identifying a U.S. person, the information must reasonably appear to be foreign intelligence or evidence of a crime, or necessary to understand or assess foreign intelligence information.

(U) **Compliance and Oversight**

(U) The Executive Branch is committed to ensuring that the Intelligence Community's use of section 702 is consistent with the law, the FISC's orders, and the protection of the privacy and civil liberties of Americans. The Intelligence Community, the Department of Justice, and the FISC all play a critical role in overseeing the use of this provision. In addition, the Intelligence and Judiciary Committees carry out essential oversight, which is discussed separately in section IV below.

~~(S//NF)~~ First, components in each agency, including operational components and agency Inspectors General, conduct extensive oversight. Agencies using section 702 authority must report promptly to the Department of Justice and to the Office of the Director of National Intelligence (ODNI) incidents of noncompliance with the targeting or minimization procedures. Members of the joint oversight team from the National Security Division (NSD) of the Department of Justice and ODNI routinely review the agencies' targeting decisions. Currently, at least once every 60 days, NSD and ODNI conduct oversight of activities under section 702. The joint oversight team evaluates and where appropriate investigates each potential incident of noncompliance, and conducts a detailed review of agencies' targeting and minimization decisions.

~~(S//NF)~~ Using the reviews by NSD and ODNI personnel, the Attorney General and the DNI assess semi-annually, as required by section 702, compliance with the targeting and minimization procedures. These assessments are provided twice yearly to Congress. In general,

the assessments have found that agencies have "continued to implement the procedures . . . in a manner that reflects a focused and concerted effort by agency personnel to comply with the requirements of Section 702." The number of compliance incidents has been small, with no indication of "any intentional attempt to circumvent or violate" legal requirements. Rather, agency personnel "are appropriately focused on directing their efforts at non-United States persons reasonably believed to be located outside the United States." *Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Submitted by the Attorney General and the Director of National Intelligence, Reporting Period: December 1, 2010 – May 31, 2011* at 2-3, 5. 21-22 (December 2011).

(U) The Intelligence Community and the Department of Justice use the reviews and oversight to evaluate whether changes to the procedures are needed, and what other steps may be appropriate under section 702 to protect the privacy of Americans. The Government also provides the joint assessments, the major portions of the semi-annual reports, and a separate quarterly report to the FISC. Taken together, these measures provide robust oversight of the Government's use of this authority.

~~(TS//SI//NF)~~ One recent event demonstrates both how this oversight regime works and how challenging collection can be in the complex and rapidly evolving Internet environment. On October 3, 2011, the FISC issued an opinion addressing the Government's submission of replacement certifications under section 702. Although the FISC upheld the bulk of the Government's submission, it denied in part the Government's requests to reauthorize the certifications because of its concerns about the rules governing the retention of certain non-targeted Internet communications -- so called multi-communication transactions or MCTs -- acquired through NSA's upstream collection. The FISC recognized, however, that the Government may be able to "tailor the scope of NSA's upstream collection, or adopt more stringent post-acquisition safeguards" in a manner that would satisfy its concerns, and suggested a number of possibilities as to how this might be done. In response to this opinion, the NSA, Department of Justice, and ODNI worked to correct the deficiencies identified by the Court. On November 30, the FISC granted the Government's request for approval of the amended procedures, stating that, with regard to information acquired pursuant to the 2011 certifications, "the government has adequately corrected the deficiencies identified in the October 3 Opinion," and that the amended procedures, when "viewed as a whole, meet the applicable statutory and constitutional requirements." These amended procedures continue to allow for the upstream collection of MCTs; however, they also create more rigorous rules governing the retention of MCTs as well as NSA analysts' exposure to, and use of, non-targeted communications. The Government's extensive efforts over several months to address this matter, and the FISC's exhaustive analysis of it, demonstrates how well the existing oversight regime works in ensuring that collection is undertaken in conformity with the statute and Court-approved procedures. This issue was also fully briefed to the appropriate congressional committees, again highlighting the important role that Congress plays in overseeing these vital intelligence activities.

(U) II. The Importance of Section 702 Collection

~~(S//NF)~~ **The Administration believes that a failure to renew this authority would result in a loss of critical foreign intelligence that cannot practicably be obtained through other methods.**

~~(S//NF)~~ To require an individualized court order, based on a finding of probable cause, before acquiring the communications of a non-U.S. person overseas who is believed to be involved in international terrorist activities or who is otherwise of foreign intelligence interest would have serious adverse consequences. Where the Intelligence Community has reason to believe that a non-U.S. person located overseas is connected to international terrorist activities, but does not have enough facts to establish probable cause to conclude that the target is acting as an agent of a foreign power, such a requirement could prevent the United States from acquiring significant intelligence. Even where the United States could, over time, amass additional information from other sources to establish probable cause, a requirement that such additional information be obtained and submitted to the FISC would result in delays in collection that could prove harmful. Second, even where the Intelligence Community has facts that establish probable cause that foreign targets are acting as foreign powers or agents of foreign powers, eliminating section 702's more flexible targeting system would significantly slow the Intelligence Community's ability to acquire important foreign intelligence information. This flexibility is critical in fast-moving threat scenarios. Significant additional resources would have to be devoted to preparing and processing the FISC applications and even then, given the number of selectors tasked, it is simply not feasible to obtain individualized orders on a routine basis for the thousands of foreign persons targeted under section 702. Intelligence would be lost. Moreover, failure to renew section 702 would require redirection of a substantial portion of the oversight resources of the Intelligence Community, the Department of Justice, and the FISC from their other important national security related work to the processing of FISA applications targeting non-U.S. persons overseas who are not entitled to Fourth Amendment protections under our Constitution. In contrast, section 702 increases the Government's ability to acquire important foreign intelligence information and to act quickly against appropriate foreign targets, without sacrificing constitutional protections for Americans.

~~(TS//SI//NF)~~ Another major benefit of section 702 is that it has made collection against foreign targets located outside the United States possible from the relative safety of collection points in the United States. [redacted]

~~(TS//SI//NF)~~ In sum, section 702 collection is a major contributor to the Intelligence Community's reporting on counterterrorism, [redacted] and other topics. Attached to this paper are several examples that demonstrate the broad range of important information that the Intelligence Community has obtained from section 702 collection.

(U) **III. Other Provisions of the FAA**

(U) In contrast to section 702, which focuses on foreign targets, section 704 addresses collection activities directed against U.S. persons overseas. Section 704 requires an individual order from the FISC in circumstances in which a U.S. person overseas has "a reasonable expectation of privacy and a warrant would be required if the acquisition were conducted inside the United States for law enforcement purposes." It also requires probable cause to believe that the targeted U.S. person is "a foreign power, an agent of a foreign power, or an officer or employee of a foreign power." Previously, these activities were outside the scope of FISA and governed exclusively by section 2.5 of Executive Order 12333.[1] By requiring the approval of the FISC, section 704 provides additional protection for civil liberties.

(U) In addition to sections 702 and 704, the FAA added several other provisions to FISA. Section 701 provides definitions for the Act. Section 703 allows the FISC to authorize an application targeting a U.S. person outside the United States where the acquisition is conducted in this country. Like section 704, section 703 requires probable cause to believe that the target is a foreign power, an agent of a foreign power, or an officer or employee of a foreign power. Section 705 allows the Government to obtain various authorities simultaneously. Section 709 clarifies that nothing in the FAA is intended to limit the Government's ability to obtain authorizations under other parts of FISA. The Government supports the reauthorization of these provisions.

(U) **IV. Congressional Oversight**

(U) The Executive Branch appreciates the need for regular and meaningful Congressional oversight of the use of section 702 and the other provisions of the FAA. Twice a year, the Attorney General must "fully inform, in a manner consistent with national security," the Intelligence and Judiciary Committees about the implementation of the FAA. Additionally, with respect to section 702, the report must include copies of certifications and directives and copies of significant pleadings and FISC opinions and orders. It also must describe compliance matters, any use of emergency authorities, and the FISC's review of the Government's pleadings. With respect to sections 703 and 704, the report must include the number of applications made, and the number granted, modified, or denied by the FISC.

(U) Section 702 also requires the Attorney General and the DNI to provide to the Intelligence and Judiciary Committees their assessment of compliance with the targeting and minimization procedures, described above. In addition, the Government has substantial reporting requirements imposed by FISA under which it has provided Congress information to ensure effective congressional oversight. The Government has informed the Intelligence and Judiciary Committees of acquisitions authorized under section 702; reported, in detail, on the results of the

[1] (U) Since before the enactment of the FAA, section 2.5 of Executive Order 12333 has required the Attorney General to approve the use by the Intelligence Community against U.S. persons abroad of "any technique for which a warrant would be required if undertaken for law enforcement purposes." The Attorney General must find that there is probable cause to believe that the U.S. person is a foreign power or an agent of a foreign power. The provisions of section 2.5 continue to apply to these activities, in addition to the requirements of section 704.

reviews and on compliance incidents and remedial efforts; made all written reports on these reviews available to the Committees; and provided summaries of significant interpretations of FISA, as well as copies of relevant judicial opinions and pleadings.

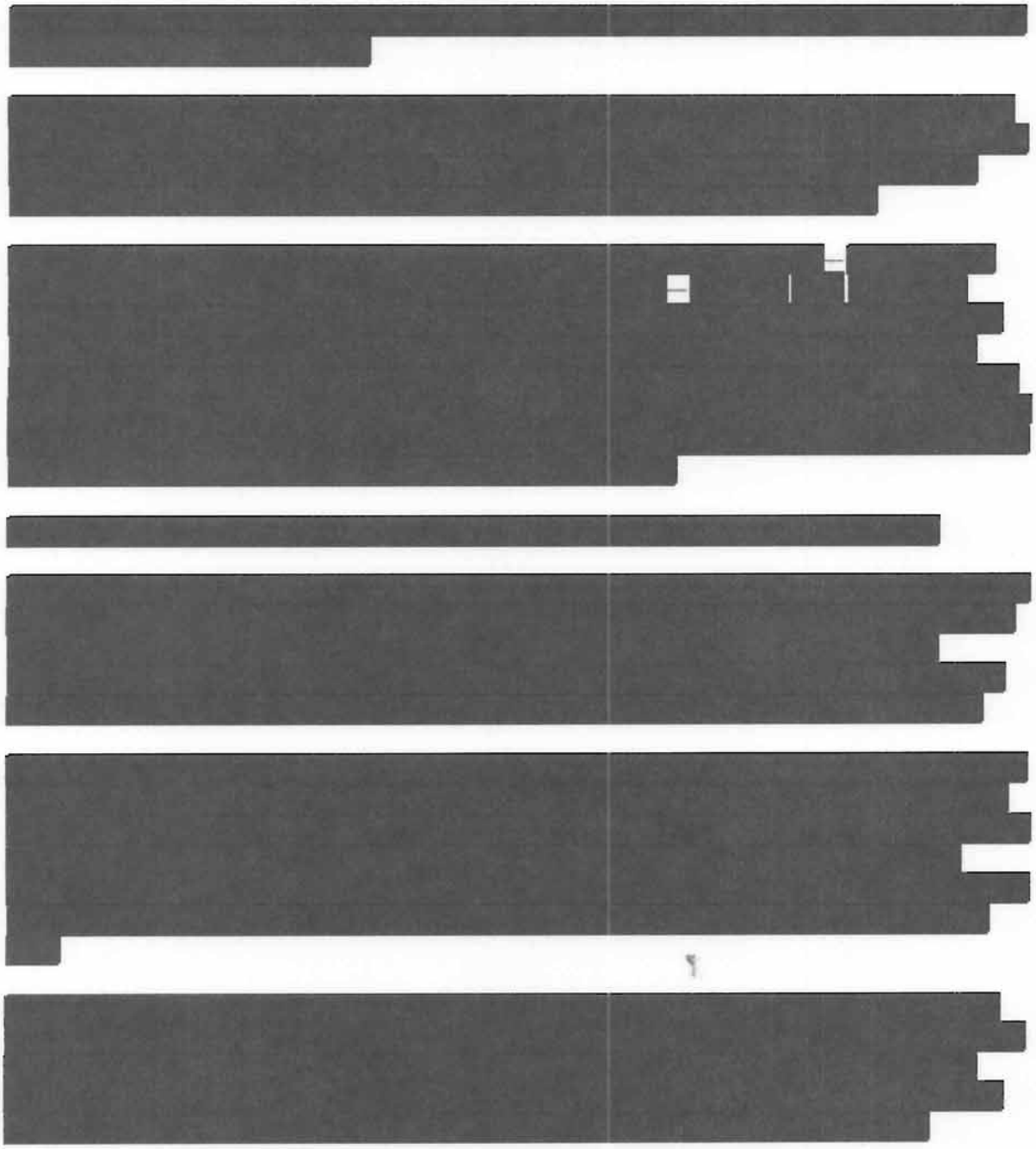
(U) **V. The Need for Reauthorization**

(U) The Administration strongly supports the reauthorization of Title VII of FISA. The FAA was the product of bipartisan effort, and its enactment was preceded by extensive public debate. There is now a lengthy factual record on the Government's need for the FAA to acquire foreign intelligence information critical to the national security. There is also a lengthy record documenting the effectiveness of the oversight process in protecting the privacy and civil liberties of Americans. This extensive record demonstrates the proven value of these authorities, and the commitment of the Government to their lawful and responsible use.

(U) Reauthorization will ensure continued certainty for the rules used by agency employees and our private partners. The Intelligence Community has invested significant human and financial resources to enable its personnel and technological systems to acquire and review vital data quickly and lawfully. Our adversaries, of course, seek to hide the most important information from us. It is at best inefficient and at worst unworkable for agencies to develop new technologies and procedures and train employees, only to have a statutory framework subject to wholesale revision. This is particularly true at a time of limited resources. We are always considering whether there are changes that could be made to improve the law in a manner consistent with the privacy and civil liberties interests of Americans. Our first priority, however, is reauthorization of these authorities in their current form. It is essential that these authorities remain in place without interruption—and without the threat of interruption—so that those who have been entrusted with their use can continue to protect our nation from its enemies.

Attachment
Value of Section 702 Collection

(U) Section 702 is a critical intelligence collection tool that has helped to protect national security. The following are "real-life" examples that demonstrate the broad range of important information that the Intelligence Community has obtained.



[redacted]

~~(S//NF)~~ **Example 4: Najibullah Zazi**

~~(S//NF)~~ The FBI's arrest in 2009 of Najibullah Zazi in Colorado, the disruption of his planned attack on the New York subway system, and his eventual guilty plea to terrorism charges were the direct result of section 702 coverage. NSA observed that an al Qa'ida external operations account, which was under section 702 coverage, sent an e-mail to Zazi in September 2009. That allowed NSA to pass Zazi's e-mail account, [redacted], and telephone number to the FBI. This initial report was based solely on section 702 collection. The report led to Zazi's identification and the discovery of purchases in Colorado that could be used in a terrorist attack, and ultimately to his arrest and the arrests of others involved in the plot. Thus section 702 facilitated the disruption of one of the most serious terrorist plots against the homeland since September 11th.

[redacted]

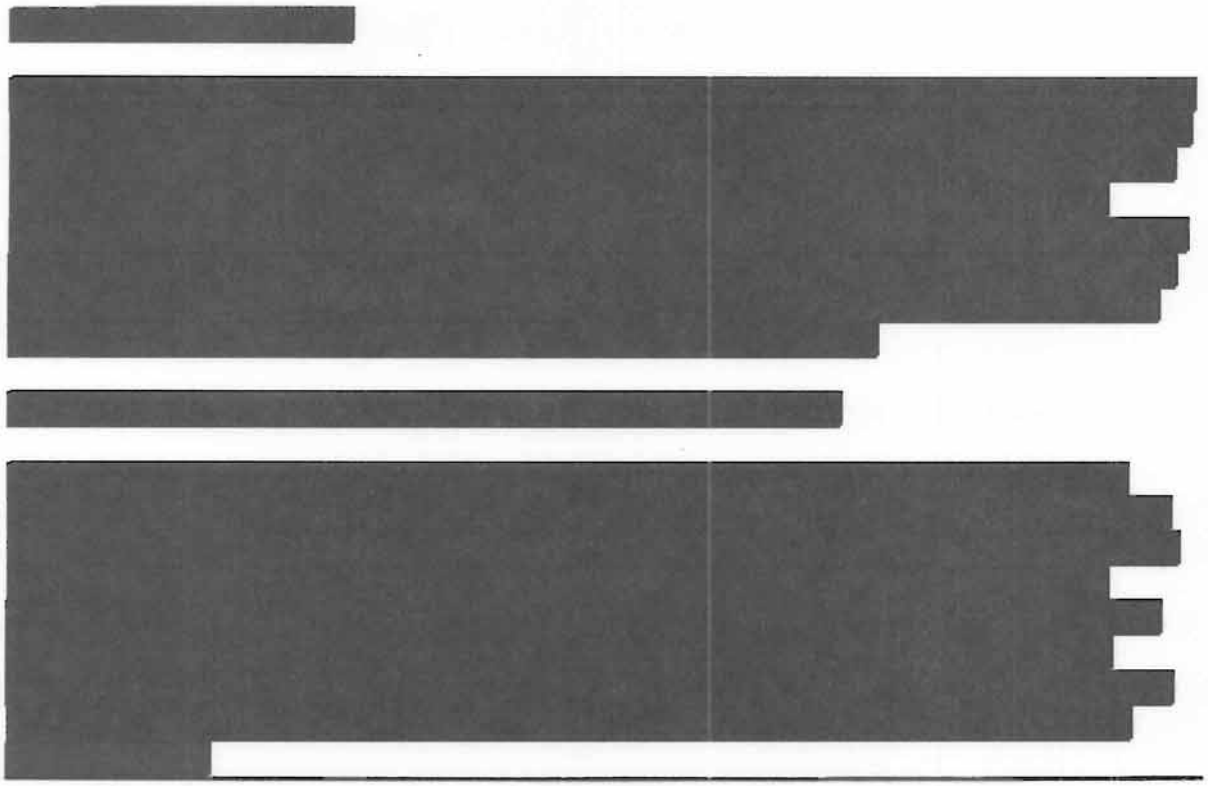


EXHIBIT C

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

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

Privacy and Civil Liberties Oversight Board

David Medine, Chairman

Rachel Brand

Elisebeth Collins Cook

James Dempsey

Patricia Wald

PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act

Part 1:

INTRODUCTION

I. Background

Shortly after the Privacy and Civil Liberties Oversight Board ("PCLOB" or "Board") began operation as a new independent agency, Board Members identified a series of programs and issues to prioritize for review. As announced at the Board's public meeting in March 2013, one of these issues was the implementation of the Foreign Intelligence Surveillance Act Amendments Act of 2008.[1]

Several months later, in June 2013, two classified National Security Agency ("NSA") collection programs were first reported about by the press based on unauthorized disclosures of classified documents by Edward Snowden, a contractor for the NSA. Under one program, implemented under Section 215 of the USA PATRIOT Act, the NSA collects domestic telephone metadata (i.e., call records) in bulk. Under the other program, implemented under Section 702 of the Foreign Intelligence Surveillance Act ("FISA"), the government collects the contents of electronic communications, including telephone calls and emails, where the target is reasonably believed to be a non-U.S. person[2] located outside the United States.

A bipartisan group of U.S. Senators asked the Board to investigate the two NSA programs and provide an unclassified report.[3] House Minority Leader Nancy Pelosi subsequently asked the Board to consider the operations of the Foreign Intelligence Surveillance Court ("FISA court").[4] Additionally, the Board met with President Obama, who asked the Board to "review where our counterterrorism efforts and our values come into

---

1 *See* Privacy and Civil Liberties Oversight Board, Minutes of Open Meeting of March 5, 2013, at 4-5, *available at* http://www.pclob.gov/SiteAssets/meetings-and-events/5-march-2013-public-meeting/5%20March%202013%20Meeting%20Minutes.pdf.

2 Under the statute, the term "U.S. persons" includes United States citizens, United States permanent residents, and virtually all United States corporations.

3 Letter from Tom Udall *et al*. to the Privacy and Civil Liberties Oversight Board (June 12, 2013), *available at* http://www.pclob.gov/SiteAssets/newsroom/6.12.13%20Senate%20letter%20to%20PCLOB.pdf. Response *available at* http://www.pclob.gov/SiteAssets/newsroom/PCLOB_TUdall.pdf.

4 Letter from Democratic Leader Nancy Pelosi to Chairman David Medine (July 11, 2013), *available at* http://www.pclob.gov/SiteAssets/newsroom/Pelosi%20Letter%20to%20PCLOB.pdf. Response *available at* http://www.pclob.gov/SiteAssets/newsroom/PCLOB%20Pelosi%20Response%20Final.pdf.

tension."[5] In response to the requests from Congress and the President, the Board began a comprehensive study of the two NSA programs. The Board held public hearings and met with the Intelligence Community and the Department of Justice, White House, and congressional committee staff, privacy and civil liberties advocates, academics, trade associations, and technology and communications companies.

During the course of this study, it became clear to the Board that each program required a level of review that was best undertaken and presented to the public in a separate report. As such, the Board released a report on the Section 215 telephone records program and the operation of the FISA court on January 23, 2014.[6] Subsequently, the Board held an additional public hearing and continued its study of the second program. Now, the Board is issuing the current report, which examines the collection of electronic communications under Section 702, and provides analysis and recommendations regarding the program's implementation.

The Section 702 program is extremely complex, involving multiple agencies, collecting multiple types of information, for multiple purposes. Overall, the Board has found that the information the program collects has been valuable and effective in protecting the nation's security and producing useful foreign intelligence. The program has operated under a statute that was publicly debated, and the text of the statute outlines the basic structure of the program. Operation of the Section 702 program has been subject to judicial oversight and extensive internal supervision, and the Board has found no evidence of intentional abuse.

The Board has found that certain aspects of the program's implementation raise privacy concerns. These include the scope of the incidental collection of U.S. persons' communications and the use of queries to search the information collected under the program for the communications of specific U.S. persons. The Board offers a series of policy recommendations to strengthen privacy safeguards and to address these concerns.

II. Study Methodology

In order to gain a full understanding of the program's operations, the Board and its staff received multiple briefings on the operation of the program, including the technical

---

5 Remarks by the President in a Press Conference at the White House (Aug. 9, 2013), *available at* http://www.whitehouse.gov/the-press-office/2013/08/09/remarks-president-press-conference.

6 *See* PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT (2014), *available at* http://www.pclob.gov/All%20Documents/Report%20on%20the%20Telephone%20Records%20Program/PCLOB-Report-on-the-Telephone-Records-Program.pdf.

target, because two non-U.S. persons are discussing a U.S. person, or because a U.S. person was mistakenly targeted. Section 702 therefore requires that certifications also include "minimization procedures" that control the acquisition, retention, and dissemination of any non–publicly available U.S. person information acquired through the Section 702 program.[74] As discussed below, the minimization procedures include different procedures for handling U.S. person information depending on the circumstances of how it was acquired. Along with the targeting procedures, the minimization procedures contain the government's core privacy and civil liberties protections and are more fully discussed throughout this Report.

C. FISC Review

The government's Section 702 certifications, targeting procedures, and minimization procedures (but not the Attorney General Guidelines) are all subject to review by the FISC.[75] In addition to the required procedures and guidelines, the Section 702 certifications are accompanied by affidavits of national security officials[76] that further describe to the FISC the government's basis for assessing that the proposed Section 702 acquisition will be consistent with the applicable statutory authorization and limits.[77] Through court filings or the testimony of witnesses at hearings before the FISC, the government also submits additional information explaining how the targeting and minimization procedures will be applied and describing the operation of the program in a way that defines its scope.[78]

The FISC's review of the Section 702 certifications has been called "limited" by scholars,[79] privacy advocates,[80] and in one instance, shortly after the FISA Amendments Act

---

74 50 U.S.C. § 1881a(e)(1), (g)(2)(A)(ii), (g)(2)(B).

75 50 U.S.C. § 1881a(d)(2), (e)(2), (i). The Attorney General Guidelines must, however, be submitted to the FISA court. 50 U.S.C. § 1881a(f)(2)(C). Section 702 does have a provision permitting the Attorney General and the Director of National Intelligence to authorize acquisition prior to judicial review of a certification under certain exigent circumstances. 50 U.S.C. § 1881a(c)(2). To date, the Attorney General and the Director of National Intelligence have never exercised this authority.

76 50 U.S.C. § 1881a(g)(2)(C); *see, e.g.*, Memorandum Opinion at 3, [*Caption Redacted*], [Docket No. Redacted], 2011 WL 10945618, at *1 (FISA Ct. Oct. 3, 2011) ("Bates October 2011 Opinion") (noting submitted affidavits by the Director or Acting Director of NSA and the Director of FBI), *available at* http://icontherecord.tumblr.com/post/58944252298/dni-declassifies-intelligence-community-documents.

77 *See* AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at A-1 to A-2.

78 *See, e.g.,* Bates October 2011 Opinion, *supra*, at 5-9, 2011 WL 10945618, at *2-4 (describing 2011 government filings with, and testimony before, the FISA court); *id*. at 15-16, 2011 WL 10945618, at *5 (describing representations made to the FISA court in prior Section 702 certifications).

79 *See, e.g.*, Laura K. Donohue, Section 702 and the Collection of International Telephone and Internet Content, at 15, 18, 30-34, *available at* http://justsecurity.org/wp-content/uploads/2014/05/donahue.702.pdf.

was passed, by the FISC itself.[81] In certain respects, this characterization is accurate. Unlike traditional FISA applications, the FISC does not review the targeting of particular individuals. Specifically, although the Section 702 certifications identify the foreign intelligence subject matters regarding which information is to be acquired, the FISC does not see or approve the specific persons targeted or the specific communication facilities that are actually tasked for acquisition. As such the government does not present evidence to the FISC, nor does the FISC determine — under probable cause or any other standard — that the particular individuals being targeted are non-U.S. persons reasonably believed to be located outside the United States who are being properly targeted to acquire foreign intelligence information.[82] Instead of requiring judicial review of these elements, Section 702 calls upon the FISA court only to decide whether the targeting procedures are reasonably designed to ensure compliance with certain limitations and that the minimization procedures satisfy certain criteria (described below). The FISC is not required to independently determine that a significant purpose of the proposed acquisition is to obtain foreign intelligence information,[83] although the foreign intelligence purpose of the collection does play a role in the court's Fourth Amendment analysis.[84]

In other respects, however, the FISC's role in the Section 702 program is more extensive. The FISC reviews both the targeting procedures and the minimization procedures, the core set of documents that implement Section 702's statutory requirements and limitations.[85] With respect to the targeting procedures, the FISC must

---

80 *See, e.g.*, Submission of Jameel Jaffer, Deputy Legal Director, American Civil Liberties Union Foundation, Privacy and Civil Liberties Oversight Board Public Hearing on Section 702 of the FISA Amendments Act, at 9 (Mar. 19, 2014), *available at* http://www.pclob.gov/Library/Meetings-Events/2014-March-19-Public-Hearing/Testimony_Jaffer.pdf.

81 Memorandum Opinion, *In re Proceedings Required by § 702(i) of the FISA Amendments Act of 2008*, Docket Misc. No. 08-01, 2008 WL 9487946, at *5 (FISA Ct. Aug. 27, 2008).

82 *See* The Intelligence Community's Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act, at 2 (2012) (describing differences between targeting individuals under traditional FISA electronic surveillance provisions and targeting pursuant to Section 702). This document accompanied a 2012 letter sent by the Department of Justice and the Office of the Director of National Intelligence to the Senate Select Committee on Intelligence and House Permanent Select Committee on Intelligence urging the reauthorization of Section 702. *See* Letter from Kathleen Turner, Director of Legislative Affairs, ODNI, and Ronald Weich, Assistant Attorney General, Office of Legislative Affairs, DOJ to the Honorable Dianne Feinstein, Chairman, Senate Committee on Intelligence, et. al. (May 4, 2012), *available at* http://www.dni.gov/files/documents/Ltr%20to%20HPSCI%20Chairman%20Rogers%20and%20Ranking%20Member%20Ruppersberger_Scan.pdf.

83 50 U.S.C. § 1881a(i)(2).

84 Additionally, if the FISC determines that a Section 702 certification and related documents are insufficient on Constitutional or statutory grounds, the FISC cannot itself modify the certification and related documents governing the Section 702 program, but instead must issue an order to the government to either correct any deficiencies identified by the FISC within 30 days or to cease (or not begin) implementation of the certification. 50 U.S.C. § 1881a(i)(3)(B).

85 50 U.S.C. § 1881a(d)(2), (e)(2), (i)(1)(A).

determine that they "are reasonably designed" to "ensure" that targeting is "limited to targeting persons reasonably believed to be located outside the United States."[86] The FISC also must determine that the targeting procedures are reasonably designed to prevent the intentional acquisition of wholly domestic communications.[87] In addition, the FISC must also review the proposed minimization procedures under the same standard of review that is required in traditional FISA electronic surveillance and physical search applications.[88] The FISC must find that such minimization procedures are "specific procedures" that are "reasonably designed" to control the acquisition, retention, and dissemination of non–publicly available U.S. person information.[89] Each time the FISC reviews a Section 702 certification, the FISC must also determine whether the proposed Section 702 acquisition as provided for, and restricted by, the targeting and minimization procedures complies with the Fourth Amendment.[90] After conducting its analysis, the FISC must issue a written opinion explaining the reasons why the court has held that the proposed targeting and minimization procedures do, or do not, comply with statutory and Fourth Amendment requirements.[91]

The FISC has held that it cannot make determinations in a vacuum regarding whether targeting and minimization procedures are "reasonably designed" to meet the statutory requirements and comply with the Fourth Amendment. To the contrary, the FISC "has repeatedly noted that the government's targeting and minimization procedures must be considered in light of the communications actually acquired," and that "[s]ubstantial implementation problems can, notwithstanding the government's intent, speak to whether the applicable targeting procedures are 'reasonably designed' to acquire only the communications of non-U.S. persons outside the United States.'"[92] Therefore, although the FISC reviews the targeting procedures, minimization procedures, and related affidavits that

---

86 50 U.S.C. § 1881a(i)(2)(B)(i).

87 50 U.S.C. § 1881a(i)(2)(B)(ii).

88 *Compare* 50 U.S.C. § 1881a(i)(2)(C) (requirement to evaluate Section 702 minimization procedures) *with* 50 U.S.C. § 1805(a)(3) (requirement to evaluate FISA electronic surveillance minimization procedures) *and* 50 U.S.C. § 1824(a)(3) (requirement to evaluate FISA physical search minimization procedures).

89 50 U.S.C. § 1801(h).

90 50 U.S.C. § 1881a(i)(3)(A), (i)(3)(B).

91 50 U.S.C. § 1881a(i)(3)(C). While FISC judges may write opinions explaining their orders with regard to other aspects of FISA, the statutory requirement for an opinion explaining the rationale of all orders approving Section 702 certifications is unique within FISA. Though not required by FISA, FISC Rule of Procedure 18(b)(1) also requires FISC judges to provide a written statement of reasons for any denials of the government's other FISA applications. *See* United States Foreign Intelligence Surveillance Court Rules of Procedure ("FISC Rule of Procedure"), Rule 18(b)(1), *available at* http://www.uscourts.gov/uscourts/rules/FISC2010.pdf.

92 Bates October 2011 Opinion, *supra*, at 28, 2011 WL 10945618, at *9 (quoting FISC opinion with redacted docket number).

are submitted with a Section 702 certification, the court's review is not limited to the four corners of those documents. The FISC also takes into consideration additional filings by the government to supplement or clarify the record, responses to FISC orders to supplement the record,[93] and the sworn testimony of witnesses at hearings.[94]

Commitments regarding how the targeting and minimization procedures will be implemented that are made to the FISC in these representations have been found to be binding on the government. For example, during the consideration of the first Section 702 certification in 2008, the government stated that that the targeting procedures impose a requirement that analysts conduct "due diligence" in determining the U.S. person status of any Section 702 target, even though the phrase "due diligence" is not explicitly found in the text of the NSA targeting procedures. The FISC incorporated the government's representation regarding due diligence into its opinion, and the government has subsequently reported to Congress and the FISC — as incidents of noncompliance — instances in which the Intelligence Community conducted insufficient due diligence that resulted in the targeting of a U.S. person.[95]

In evaluating the Section 702 certifications, the court also considers additional filings required by the FISC's Rules of Procedure. One such rule requires the government to notify the FISA court whenever the government discovers a material misstatement or omissions in a prior filing with the court.[96] Another rule mandates that the government report to the FISA court incidents of noncompliance with targeting or minimization procedures previously approved by the court.[97] In a still-classified 2009 opinion, the FISC held that the judicial review requirements regarding the targeting and minimization procedures required that the FISC be fully informed of every incident of noncompliance

---

93 *See* FISC Rule of Procedure 5(c) (stating that the FISC Judges have the authority to order any party to a proceeding to supplement the record by "furnish[ing] any information that the Judge deems necessary").

94 FISC Rule of Procedure 17.

95 *See* AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 29 (describing incidents and stating "In each of these incidents, all Section 702–acquired data was purged. Together, these [redacted] instances represent isolated instances of insufficient due diligence that do not reflect the [redacted] of taskings that occur during the reporting period.").

96 *See* FISC Rule of Procedure 13(a).

97 *See* FISC Rule of Procedure 13(b); SEMIANNUAL ASSESSMENT OF COMPLIANCE WITH PROCEDURES AND GUIDELINES ISSUES PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, MAY 2010, at 22 ("MAY 2010 SEMIANNUAL ASSESSMENT") (discussing requirements under Rule 10(c), the predecessor to Rule 13(b) in the prior set of FISC Rules of Procedure), *available at* http://www.dni.gov/files/documents/FAA/SAR%20May%202010%20Final%20Release%20with%20Exemptions.pdf. The government also provides the FISC the Semiannual Section 702 Joint Assessment, portions of the Section 707 Semiannual report, and a separate quarterly report to the FISC, all of which describe scope, nature, and actions taken in response to compliance incidents. *See* The Intelligence Community's Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act, *supra*, at 5; 50 U.S.C. § 1881a(l)(1).

with those procedures. In the 2009 opinion, the court analyzed whether several errors in applying the targeting and minimization procedures that had been reported to the court undermined either the court's statutory or constitutional analysis. (The court concluded that they did not.)

In addition to identifying errors that could impact the sufficiency of the targeting and minimization procedures, these compliance notices play an additional role in informing the FISC regarding how the government is in fact applying the targeting and minimization procedures. Specifically, the compliance notices must state both the type of noncompliance that has occurred and the facts and circumstances relevant to the incident.[98] In doing so, representations to the FISA court have in essence created a series of precedents regarding how the government is interpreting various provisions of its targeting and minimization procedures, which informs the court's conclusions regarding whether those procedures — as actually applied by the Intelligence Community to particular, real-life factual scenarios — comply with Section 702's statutory requirements and the Fourth Amendment. For example, while the 2008 FISC opinion incorporated the government's commitment to apply due diligence in determining the U.S. person status of potential targets, notices of non-compliance filed by the government reflect that the government interprets the targeting procedures to also require due diligence in determining the *location* of potential targets. Similarly, the government has filed letters clarifying aspects of its "post-tasking" process, which are discussed further below, and it has reported — as compliance incidents — instances when its performance of the post-tasking process has not complied with those representations. The government's interpretations of the targeting and minimization procedures reflected in these compliance filings, however, are not necessarily formally endorsed or incorporated into the FISC's subsequent opinions. In the Board's opinion Intelligence Community personnel applying these procedures months or years later may not be aware of the interpretive gloss arising from prior interactions between the government and the FISC on these procedures.

Former FISC Presiding Judge John Bates' October 3, 2011 opinion provides both an example of the scope of the FISA court's review of Section 702 certifications in practice and an illustration of what actions the court can take if it determines that the government has not satisfied the court's expectations to be kept fully, accurately, and timely informed. In April 2011, the government filed multiple Section 702 certifications with the FISC.[99] In early May 2011, however, the government filed a letter with the court (under a FISC procedural rule regarding material misstatements or omissions) acknowledging that the scope of the NSA's "upstream" collection (described below) was more expansive than

---

98 FISC Rule of Procedure 13(b).

99 Bates October 2011 Opinion, *supra*, at 3, 2011 WL 10945618, at *1.

previously represented to the court.[100] As a result of the filing, the FISC expressed serious concern that the upstream collection, as described by the government, may have exceeded the scope of collection previously approved by the FISC and what could be authorized under Section 702. The FISC therefore ordered the government to respond to a number of questions regarding the upstream collection program.[101] Throughout the summer of 2011, the government continued to supplement the record in response to the FISA court's concerns with a number of filings, including by conducting and reporting to the court the results of a statistical sample of the NSA's acquisition of upstream collection.[102] The government's supplemental filings discussed both factual matters, such as how many domestic communications were being acquired as a result of the manner in which the government was conducting upstream collection, as well as the government's legal interpretations regarding how the NSA's minimization procedures should be applied to such acquisition.[103] The FISA court also met with the government and held a hearing to ask additional questions of NSA and Department of Justice personnel.[104]

Based on this record, Judge Bates ultimately held that in light of the new information, portions of the NSA minimization procedures met neither the requirements of FISA nor the Fourth Amendment and ordered the government to correct the deficient procedures or cease Section 702 upstream collection.[105] The government subsequently modified the NSA minimization procedures to remedy the deficiencies identified by the FISA court.[106] The FISC continued to have questions, however, regarding upstream collection that had been acquired prior to the implementation of these modified NSA minimization procedures.[107] The government took several actions with regard to this past upstream collection, and ultimately decided to purge it all.[108]

---

100 Bates October 2011 Opinion, *supra*, at 5, 2011 WL 10945618, at *2.

101 Bates October 2011 Opinion, *supra*, at 7, 2011 WL 10945618, at *2.

102 Bates October 2011 Opinion, *supra*, at 10, 2011 WL 10945618, at *3-4.

103 Bates October 2011 Opinion, *supra*, at 33-35, 50, 54-56, 2011 WL 10945618, at *11, *17, *18-19.

104 Bates October 2011 Opinion, *supra*, at 7-9, 2011 WL 10945618, at *4.

105 Bates October 2011 Opinion, *supra*, at 59-63, 67-80, 2011 WL 10945618, at *20-28.

106 *See generally* Memorandum Opinion, [*Caption Redacted*], [Docket No. Redacted], 2011 WL 10947772 (FISA Ct. Nov. 30, 2011) ("Bates November 2011 Opinion"), *available at* http://icontherecord.tumblr.com/post/58944252298/dni-declassifies-intelligence-community-documents.

107 *See* Memorandum Opinion at 26-30, [*Caption Redacted*], [Docket No. Redacted], 2012 WL 9189263, at *1-4 (FISA Ct. Sept. 25, 2012) ("Bates September 2012 Opinion"), *available at* http://www.dni.gov/files/documents/September%202012%20Bates%20Opinion%20and%20Order.pdf.

108 Bates September 2012 Opinion, *supra*, at 30-32, 2012 WL 9189263, at *3-4.

D. Directives

As noted above, Section 702 targeting may occur only with the assistance of electronic communication service providers. Once Section 702 acquisition has been authorized, the Attorney General and the Director of National Intelligence send written directives to electronic communication service providers compelling the providers' assistance in the acquisition.[109] Providers that receive a Section 702 directive may challenge the legality of the directive in the FISC.[110] The government may likewise file a petition with the FISC to compel a provider that does not comply with a directive to assist the government's acquisition of foreign intelligence information.[111] The FISC's decisions regarding challenges and enforcement actions regarding directives are appealable to the Foreign Intelligence Surveillance Court of Review ("FISCR"), and either the government or a provider may request that the United States Supreme Court review a decision of the FISCR.[112]

III. Acquisition Process: How Does Section 702 Surveillance Actually Work?

Once a Section 702 certification has been approved, non-U.S. persons reasonably believed to be located outside the United States may be targeted to acquire foreign intelligence information within the scope of that certification. The process by which non-U.S. persons are targeted is detailed in the next section. This section describes how Section 702 acquisition takes place once an individual has been targeted.

A. Targeting Persons by Tasking Selectors

The Section 702 certifications permit non-U.S. persons to be targeted only through the "tasking" of what are called "selectors." A selector must be a specific communications facility that is assessed to be used by the target, such as the target's email address or telephone number.[113] Thus, in the terminology of Section 702, people (non-U.S. persons reasonably believed to be located outside the United States) are *targeted*; selectors (e.g., email addresses, telephone numbers) are *tasked*. The users of any tasked selector are

---

109 50 U.S.C. § 1881a(h).

110 50 U.S.C. § 1881a(h)(4).

111 50 U.S.C. § 1881a(h)(5).

112 50 U.S.C. § 1881a(h)(6). However, as noted in the Board's Section 215 report, to date, only two cases have been appealed to the FISCR. One, *In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act,* 551 F.3d 1004 (FISA Ct. Rev. 2008), involved a directive under the Protect America Act, the predecessor to Section 702, but none have involved Section 702. Nor has the U.S. Supreme Court ever considered the merits of a FISA order or ruled on the merits of any challenge to FISA.

113 *See* AUGUST 2013 JOINT ASSESSMENT, *supra*, at A-2; NSA DCLPO REPORT, *supra*, at 4; The Intelligence Community's Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act, *supra*, at 3.

considered targets — and therefore only selectors used by non-U.S. persons reasonably believed to be located abroad may be tasked. The targeting procedures govern both the targeting and tasking process.

Because such terms would not identify specific communications facilities, selectors may not be key words (such as "bomb" or "attack"), or the names of targeted individuals ("Osama Bin Laden").[114] Under the NSA targeting procedures, if a U.S. person or a person located in the United States is determined to be a user of a selector, that selector may not be tasked to Section 702 acquisition or must be promptly detasked if the selector has already been tasked.[115]

Although targeting decisions must be individualized, this does not mean that a substantial number of persons are not targeted under the Section 702 program. The government estimates that 89,138 persons were targeted under Section 702 during 2013.[116]

Once a selector has been tasked under the targeting procedures, it is sent to an electronic communications service provider to begin acquisition. There are two types of Section 702 acquisition: what has been referred to as "PRISM" collection and "upstream" collection. PRISM collection is the easier of the two acquisition methods to understand.

B. PRISM Collection

In PRISM collection, the government (specifically, the FBI on behalf of the NSA) sends selectors — such as an email address — to a United States–based electronic communications service provider (such as an Internet service provider, or "ISP") that has been served a directive.[117] Under the directive, the service provider is compelled to give the communications sent to or from that selector to the government (but not communications that are only "about" the selector, as described below).[118] As of mid-2011, 91 percent of the

---

114 NSA DCLPO REPORT, *supra*, at 4; PCLOB March 2014 Hearing Transcript, *supra*, at 57 (statement of Rajesh De, General Counsel, NSA) (noting that a name cannot be tasked).

115 NSA DCLPO REPORT, *supra*, at 6.

116 OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE STATISTICAL TRANSPARENCY REPORT REGARDING USE OF NATIONAL SECURITY AUTHORITIES: ANNUAL STATISTICS FOR CALENDAR YEAR 2013, at 1 (June 26, 2014), a*vailable at* http://www.dni.gov/files/tp/National_Security_Authorities_Transparency_Report_CY2013.pdf. In calculating this estimate, the government counted two known people using one tasked email address as two targets and one person known to use two tasked email addresses as one target. The number of targets is an estimate because the government may not be aware of all of the users of a particular tasked selector.

117 The Intelligence Community's Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act, *supra*, at 3. *See also* PCLOB March 2014 Hearing Transcript at 70 (statement of Rajesh De, General Counsel, NSA) (noting any recipient company "would have received legal process").

118 PCLOB March 2014 Hearing Transcript at 70; *see also* NSA DCLPO REPORT, *supra*, at 5.

Internet communications that the NSA acquired each year were obtained through PRISM collection.[119]

The government has not declassified the specific ISPs that have been served directives to undertake PRISM collection, but an example using a fake United States company ("USA-ISP Company") may clarify how PRISM collection works in practice: The NSA learns that John Target, a non-U.S. person located outside the United States, uses the email address "johntarget@usa-ISP.com" to communicate with associates about his efforts to engage in international terrorism. The NSA applies its targeting procedures (described below) and "tasks" johntarget@usa-ISP.com to Section 702 acquisition for the purpose of acquiring information about John Target's involvement in international terrorism. The FBI would then contact USA-ISP Company (a company that has previously been sent a Section 702 directive) and instruct USA-ISP Company to provide to the government all communications to or from email address johntarget@usa-ISP.com. The acquisition continues until the government "detasks" johntarget@usa-ISP.com.

The NSA receives all PRISM collection acquired under Section 702. In addition, a copy of the raw data acquired via PRISM collection — and, to date, only PRISM collection — may also be sent to the CIA and/or FBI.[120] The NSA, CIA, and FBI all must apply their own minimization procedures to any PRISM-acquired data.[121]

Before data is entered into systems available to trained analysts or agents, government technical personnel use technical systems to help verify that data sent by the provider is limited to the data requested by the government. To again use the John Target example above, if the NSA determined that johntarget@usa-ISP.com was not actually going to be used to communicate information about international terrorism, the government would send a detasking request to USA-ISP Company to stop further Section 702 collection on this email address. After passing on the detasking request to USA-ISP Company, the government would use its technical systems to block any further Section 702 acquisition from johntarget@usa-ISP.com to ensure that Section 702 collection against this address was immediately terminated.

---

119 Bates October 2011 Opinion, *supra*, at 29-30 and n.24, 2011 WL 10945618, at *25 & n.24.

120 Minimization Procedures used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended, § 6(c) (Oct. 31, 2011) ("NSA 2011 Minimization Procedures"), *available at* http://www.dni.gov/files/documents/Minimization%20Procedures%20used%20by%20NSA%20in%20Connection%20with%20FISA%20SECT%20702.pdf.

121 NSA 2011 Minimization Procedures, *supra*, § 6(c).

C. Upstream Collection

The NSA acquires communications from a second means, which is referred to as upstream collection. Upstream collection is different from PRISM collection because the acquisition occurs not with the compelled assistance of the United States ISPs, but instead with the compelled assistance (through a Section 702 directive) of the providers that control the telecommunications backbone over which communications transit.[122] The collection therefore does not occur at the local telephone company or email provider with whom the targeted person interacts (which may be foreign telephone or Internet companies, which the government cannot compel to comply with a Section 702 directive), but instead occurs "upstream" in the flow of communications between communication service providers.[123]

Unlike PRISM collection, raw upstream collection is not routed to the CIA or FBI, and therefore it resides only in NSA systems, where it is subject to the NSA's minimization procedures. [124] CIA and FBI personnel therefore lack any access to raw data from upstream collection. Accordingly, they cannot view or query such data in CIA or FBI systems.

The upstream acquisition of telephone and Internet communications differ from each other, and these differences affect privacy and civil liberty interests in varied ways.[125] Each type of Section 702 upstream collection is discussed below. In conducting both types of upstream acquisition, NSA employs certain collection monitoring programs to identify anomalies that could indicate that technical issues in the collection platform are causing data to be overcollected.[126]

---

122 The Intelligence Community's Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act, *supra*, at 3-4; *see also* PCLOB March 2014 Hearing Transcript, *supra*, at 26 (statement of Rajesh De, General Counsel, NSA) ("The second type of collection is the shorthand referred to as upstream collection. Upstream collection refers to collection from the, for lack of a better phrase, Internet backbone rather than Internet service providers.").

123 *See* PCLOB March 2014 Hearing Transcript, *supra*, at 26 (statement of Rajesh De, General Counsel, NSA) ("This type of collection upstream fills a particular gap of allowing us to collect communications that are not available under PRISM collection.").

124 The Intelligence Community's Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act, *supra*, at 4.

125 *See* PCLOB March 2014 Hearing Transcript, *supra*, at 27 (statement of Rajesh De, General Counsel, NSA).

126 AUGUST 2013 SEMIANNUAL ASSESSMENT, *supra*, at 29.

1. Upstream Collection of Telephone Communications

Like PRISM collection, the upstream collection of telephone communications begins with the NSA's tasking of a selector.[127] The same targeting procedures that govern the tasking of an email address in PRISM collection also apply to the tasking of a telephone number in upstream collection.[128] Prior to tasking, the NSA therefore is required to assess that the specific telephone number to be tasked is used by a non-U.S. person reasonably believed to be located outside the United States from whom the NSA assesses it may acquire the types of foreign intelligence information authorized under one of the Section 702 certifications. Once the targeting procedures have been applied, the NSA sends the tasked telephone number to a United States electronic communication service provider to initiate acquisition.[129] The communications acquired, with the compelled assistance of the provider, are limited to telephone communications that are either to or from the tasked telephone number that is used by the targeted person. Upstream telephony collection therefore does not acquire communications that are merely "about" the tasked telephone number.[130]

2. Upstream Collection of Internet "Transactions"

The process of tasking selectors to acquire Internet transactions is similar to tasking selectors to PRISM and upstream telephony acquisition, but the actual acquisition is substantially different. Like PRISM and upstream telephony acquisition, the NSA may only target non-U.S. persons by tasking specific selectors to upstream Internet transaction collection.[131] And, like other forms of Section 702 collection, selectors tasked for upstream Internet transaction collection must be specific selectors (such as an email address), and may not be key words or the names of targeted individuals.[132]

Once tasked, selectors used for the acquisition of upstream Internet transactions are sent to a United States electronic communication service provider to acquire communications that are transiting through circuits that are used to facilitate Internet

---

127 PCLOB March 2014 Hearing Transcript, *supra*, at 26 (statement of Rajesh De, General Counsel, NSA); *id*. at 51-53 (statement of Brad Wiegmann, Deputy Assistant Attorney General, National Security Division, DOJ).

128 NSA DCLPO REPORT, *supra*, at 6.

129 PCLOB March 2014 Hearing Transcript, *supra*, at 53-54 (statements of Rajesh De, General Counsel, NSA, and Brad Wiegmann, Deputy Assistant Attorney General, National Security Division, DOJ).

130 Bates October 2011 Opinion, *supra*, at 15, 2011 WL 10945618, at *5.

131 NSA DCLPO REPORT, *supra*, at 5-6.

132 NSA DCLPO REPORT, *supra*, at 4; PCLOB March 2014 Hearing Transcript, *supra*, at 57 (statement of Rajesh De, General Counsel, NSA) (noting that a name cannot be tasked).

communications, what is referred to as the "Internet backbone."[133] The provider is compelled to assist the government in acquiring communications across these circuits. To identify and acquire Internet transactions associated with the Section 702–tasked selectors on the Internet backbone, Internet transactions are first filtered to eliminate potential domestic transactions, and then are screened to capture only transactions containing a tasked selector. Unless transactions pass both these screens, they are not ingested into government databases. As of 2011, the NSA acquired approximately 26.5 million Internet transactions a year as a result of upstream collection.[134]

Upstream collection acquires Internet transactions that are "to," "from," or "about" a tasked selector.[135] With respect to "to" and "from" communications, the sender or a recipient is a user of a Section 702–tasked selector. This is not, however, necessarily true for an "about" communication. An "about" communication is one in which the tasked selector is referenced within the acquired Internet transaction, but the target is not necessarily a participant in the communication.[136] If the NSA therefore applied its targeting procedures to task email address "JohnTarget@example.com," to Section 702 upstream collection, the NSA would potentially acquire communications routed through the Internet backbone that were sent from email address JohnTarget@example.com, that were sent to JohnTarget@example.com, and communications that mentioned JohnTarget@example.com in the body of the message. The NSA would not, however, acquire communications simply because they contained the name "John Target." In a still-classified September 2008 opinion, the FISC agreed with the government's conclusion that the government's target when it acquires an "about" communication is not the sender or recipients of the communication, regarding whom the government may know nothing, but instead the targeted user of the Section 702–tasked selector. The FISC's reasoning relied upon language in a congressional report, later quoted by the FISA Court of Review, that the

---

133 The Intelligence Community's Collection Programs Under Title VII of the Foreign Intelligence Surveillance Act, *supra*, at 3-4.

134 Bates October 2011 Opinion, *supra*, at 73, 2011 WL 10945618, at *26.

135 *See, e.g.*, October 2011 Opinion, *supra*, at 15-16, 2011 WL 10945618, at *5-6 (describing the government's representations regarding upstream collection in the first Section 702 certification the FISC reviewed).

136 Bates October 2011 Opinion, *supra*, at 15, 2011 WL 10945618, at *5; Joint Statement of Lisa O. Monaco, Assistant Attorney General, National Security Division, Dept. of Justice, et. al., *Hearing Before the House Permanent Select Comm. on Intelligence: FISA Amendments Act Reauthorization*, at 7 (Dec. 8, 2011) ("December 2011 Joint Statement") (statement of Brad Wiegmann, Deputy Assistant Attorney General, National Security Division, DOJ), *available at* http://www.dni.gov/files/documents/Joint%20Statement%20FAA%20Reauthorization%20Hearing%20-%20December%202011.pdf; PCLOB March 2014 Hearing Transcript, *supra*, at 55.

privacy intrusion even in the absence of abuse, and a number of the Board's recommendations are motivated by a desire to provide more clarity and transparency regarding the government's activities in the Section 702 program.

II. Value of the Section 702 Program

A. Advantages and Unique Capabilities

The Section 702 program makes a substantial contribution to the government's efforts to learn about the membership, goals, and activities of international terrorist organizations, and to prevent acts of terrorism from coming to fruition. Section 702 allows the government to acquire a greater range of foreign intelligence than it otherwise would be able to obtain, and it provides a degree of flexibility not offered by comparable surveillance authorities.

Because the oversight mandate of the Board extends only to those measures taken to protect the nation from terrorism, our focus in this section is limited to the counterterrorism value of the Section 702 program, although the program serves a broader range of foreign intelligence purposes.[457]

Section 702 enables the government to acquire the contents of international telephone and Internet communications in pursuit of foreign intelligence. While this ability is to some degree provided by other legal authorities, particularly "traditional" FISA and Executive Order 12333, Section 702 offers advantages over these other authorities.

In order to conduct electronic surveillance under "traditional" FISA (i.e., Title I of the Foreign Intelligence Surveillance Act of 1978), the government must persuade the Foreign Intelligence Surveillance Court ("FISC" or "FISA court"), under a standard of probable cause, that an individual it seeks to target for surveillance is an agent of a foreign power, and that the telephone number or other communications facility it seeks to monitor is used, or is about to be used, by a foreign power or one of its agents.[458] In addition, a high-level executive branch official must certify (with a supporting statement of facts) that a significant purpose of the surveillance is to obtain foreign intelligence, and that the information sought cannot reasonably be obtained through normal investigative techniques.[459] To meet these requirements and satisfy the probable cause standard, facts must be gathered by the Intelligence Community, a detailed FISA court application must be drafted by the DOJ, the facts in the application must be vetted for accuracy, the senior

---

457 See page 25 of this Report.

458 50 U.S.C. § 1805(a)(2).

459 50 U.S.C. § 1804(a)(6).

government official's certification must be prepared, the Attorney General must approve the application, and the application must be submitted to the FISA court, which must review it, determine if the pertinent standards are met, and, if so, grant it.[460] These steps consume significant time and resources.[461] In practice, FISA applications are lengthy and the process not infrequently takes weeks from beginning to final approval.[462]

This system is deliberately rigorous, for it was designed to provide a check on the government's surveillance of U.S. persons and other people located in the United States. Its goal was to prevent the abusive and politically motivated surveillance of U.S. persons and domestic activists that had occurred under the guise of foreign intelligence surveillance in the mid-twentieth century. Under FISA, electronic surveillance may be directed only at individuals who are acting at the behest of a foreign power (such as a foreign government or international terrorist organization), only for legitimate foreign intelligence purposes, and only where the aims of the surveillance cannot be achieved by other means.[463] The statute's procedural hurdles help to ensure that surveillance takes place only after detailed analysis, a strong factual showing, measured judgment by high-level executive branch officials, and approval by a neutral judge.

Although the FISA process was designed for surveillance directed at people located in the United States, the government later sought and obtained approval from the FISA court to use this process to target foreign persons located outside the United States as well. Developments in communications technology and the Internet services industry meant that such surveillance could feasibly be conducted from within the United States in some instances.[464] Utilizing the process of traditional FISA to target significant numbers of individuals overseas, however, required considerable time and resources, and government officials have argued that it slowed and sometimes prevented the acquisition of important intelligence.[465]

---

460 *See* 50 U.S.C. §§ 1804, 1805.

461 These steps also must be repeated each time the government wishes to continue the surveillance beyond the time limit specified in the original order. *See* 50 U.S.C. § 1805(d).

462 FISA permits surveillance to begin prior to court approval in emergency situations, but in order to exercise this option the Attorney General must make a determination that an emergency exists and that the factual basis required for the surveillance exists, and an application must be submitted to the FISA court for the normal probable cause determination within seven days. *See* 50 U.S.C. § 1805(e).

463 Moreover, when the target of surveillance is a U.S. person, that person must be "knowingly" acting on behalf of a foreign power. *See* 50 U.S.C. § 1801(b)(1), (2). An exception to the requirement that the target be acting on behalf of a foreign power permits a so-called "lone wolf" with no apparent connection to a foreign power to be targeted, if there is probable cause that the person is engaged in international terrorism or proliferation of weapons of mass destruction. *See* 50 U.S.C. §§ 1801(b)(1)(C), (D), 1805(a)(2)(A).

464 See pages 16-18 of this Report.

465 See pages 18-19 of this Report.

Section 702 imposes significantly fewer limits on the government when it targets non–U.S. persons located abroad, permitting greater flexibility and a dramatic increase in the number of people who can realistically be targeted.[466] Rather than approving or denying individual targeting requests, the FISA court authorizes the surveillance program as a whole, approving the certification in which the government identifies the types of foreign intelligence information sought and the procedures the government uses to target people and handle the information it obtains.[467] Targets of surveillance need not be agents of foreign powers; instead, the government may target any non-U.S. person overseas whom it reasonably believes has or is likely to communicate designated types of foreign intelligence.[468] The government need not have probable cause for this belief, or for its belief that the target uses the particular selector, such as a telephone number or email address, to be monitored. There is no requirement that the information sought cannot be acquired through normal investigative techniques. Targeting decisions are made by NSA analysts and reviewed only within the executive branch.[469] Once monitoring of a particular person begins, it may continue until new information indicates that the person no longer is an appropriate target. Whether a person remains a valid target must be reviewed annually.[470]

These differences allow the government to target a much wider range of foreigners than was possible under traditional FISA. For instance, people who might have knowledge about a suspected terrorist can be targeted even if those people are not themselves involved in terrorism or any illegitimate activity.

In addition to expanding the pool of potential surveillance targets, Section 702 also enables a much greater degree of flexibility, allowing the government to quickly begin monitoring new targets and communications facilities without the delay occasioned by the requirement to secure approval from the FISA court for each targeting decision.

As a result of these two factors, the number of people who can feasibly be targeted is significantly greater under Section 702 than under the traditional FISA process. And

---

466 Under FISA and the FISA Amendments Act, the term "United States person" includes U.S. citizens, legal permanent residents, unincorporated associations with a substantial number of U.S. citizens or legal permanent residents as members, and corporations incorporated in the United States. It does not include associations or corporations that qualify as a "foreign power." *See* 50 U.S.C. § 1801(i).

467 50 U.S.C. § 1881a(a), (i).

468 NSA DIRECTOR OF CIVIL LIBERTIES AND PRIVACY OFFICE REPORT: NSA'S IMPLEMENTATION OF FOREIGN INTELLIGENCE SURVEILLANCE ACT SECTION 702, at 4 (April 16, 2014) ("NSA DCLPO REPORT"), *available at* http://www.dni.gov/files/documents/0421/702%20Unclassified%20Document.pdf.

469 NSA DCLPO REPORT, *supra*, at 4-5.

470 Analysts are required to review the communications acquired from a target at least annually, to ensure that the targeting is still expected to provide the foreign intelligence sought and that the person otherwise remains an appropriate target under Section 702. *See* NSA DCLPO REPORT, *supra*, at 6.

indeed, the number of targets under the program has been steadily increasing since the statute was enacted in 2008.

The government also conducts foreign intelligence surveillance outside of the United States against non-U.S. persons under the authority of Executive Order 12333. In some instances, this surveillance can capture the same communications that the government obtains within the United States through Section 702. And because this collection takes place outside the United States, it is not restricted by the detailed rules of FISA outlined above.[471] Nevertheless, Section 702 offers advantages over Executive Order 12333 with respect to electronic surveillance. The fact that Section 702 collection occurs in the United States, with the compelled assistance of electronic communications service providers, contributes to the safety and security of the collection, enabling the government to protect its methods and technology. In addition, acquiring communications with the compelled assistance of U.S. companies allows service providers and the government to manage the manner in which the collection occurs. By helping to prevent incidents of overcollection and swiftly remedy problems that do occur, this arrangement can benefit the privacy of people whose communications are at risk of being acquired mistakenly.

B. Contributions to Counterterrorism

The Section 702 program has proven valuable in a number of ways to the government's efforts to combat terrorism. It has helped the United States learn more about the membership, leadership structure, priorities, tactics, and plans of international terrorist organizations. It has enabled the discovery of previously unknown terrorist operatives as well as the locations and movements of suspects already known to the government. It has led to the discovery of previously unknown terrorist plots directed against the United States and foreign countries, enabling the disruption of those plots.

While the Section 702 program is indeed a *program*, operating to some degree as a cohesive whole and approved by the FISA court accordingly, its implementation consists entirely of targeting specific individuals about whom the government already knows something. Because surveillance is conducted on an individualized basis where there is reason to target a particular person, it is perhaps unsurprising that the program yields a great deal of useful information.

The value of the Section 702 program is to some extent reflected in the breadth of NSA intelligence reporting based on information derived from the program. Since 2008, the number of signals intelligence reports based in whole or in part on Section 702 has

---

471 FISA does not generally cover surveillance conducted outside the United States, except where the surveillance intentionally targets a particular, known U.S. person, or where it acquires radio communications in which the sender and all intended recipients are located in the United States and the acquisition would require a warrant for law enforcement purposes. *See* 50 U.S.C. §§ 1801(f), 1881c.

increased exponentially. A significant portion of those reports relate to counterterrorism, and the NSA disseminates hundreds of reports per month concerning terrorism that include information derived from Section 702. Presently, over a quarter of the NSA's reports concerning international terrorism include information based in whole or in part on Section 702 collection, and this percentage has increased every year since the statute was enacted. These reports are used by the recipient agencies and departments for a variety of purposes, including to inform senior leaders in government and for operational planning.

More concretely, information acquired from Section 702 has helped the Intelligence Community to understand the structure and hierarchy of international terrorist networks, as well as their intentions and tactics. In even the most well-known terrorist organizations, only a small number of individuals have a public presence. Terrorist groups use a number of practices to obscure their membership and activities. Section 702 has enabled the U.S. government to monitor these terrorist networks in order to learn how they operate and to understand how their priorities, strategies, and tactics continue to evolve.

Monitoring these networks under Section 702 has led the government to identify previously unknown individuals who are involved in international terrorism. Identifying such persons allows the government to pursue new efforts focusing on those individuals and the disruption of their activities, such as taking action to prevent them from entering the United States. Finally, the flexibility of Section 702 surveillance enables the government to effectively maintain coverage on particular individuals as they add or switch their modes of communications.

As important as discovering the identities of individuals engaged in international terrorism is determining where those individuals are located. Modern communications permit the members of a terrorist group, and even a small number of people involved in a specific plot, to be spread out all over the world. Information acquired from Section 702 has been used to monitor individuals believed to be engaged in terrorism.

In one case, for example, the NSA was conducting surveillance under Section 702 of an email address used by an extremist based in Yemen. Through that surveillance, the agency discovered a connection between that extremist and an unknown person in Kansas City, Missouri. The NSA passed this information to the FBI, which identified the unknown person, Khalid Ouazzani, and subsequently discovered that he had connections to U.S.-based Al Qaeda associates, who had previously been part of an abandoned early stage plot to bomb the New York Stock Exchange. All of these individuals eventually pled guilty to providing and attempting to provide material support to Al Qaeda.

Finally, pursuit of the foregoing information under Section 702 has led to the discovery of previously unknown terrorist plots and has enabled the government to

disrupt them. By providing the sites of specific targets of attacks, the means being contemplated to carry out the attacks, and the identities and locations of the participants, the Section 702 program has directly enabled the thwarting of specific terrorist attacks, aimed at the United States and at other countries.

For instance, in September 2009, the NSA monitored under Section 702 the email address of an Al Qaeda courier based in Pakistan. Through that collection, the agency intercepted emails sent to that address from an unknown individual located in the United States. Despite using language designed to mask their true intent, the messages indicated that the sender was urgently seeking advice on the correct mixture of ingredients to use for making explosives. The NSA passed this information to the FBI, which used a national security letter to identify the unknown individual as Najibullah Zazi, located near Denver, Colorado. The FBI then began intense monitoring of Zazi, including physical surveillance and obtaining legal authority to monitor his Internet activity. The Bureau was able to track Zazi as he left Colorado a few days later to drive to New York City, where he and a group of confederates were planning to detonate explosives on subway lines in Manhattan within the week. Once Zazi became aware that law enforcement was tracking him, he returned to Colorado, where he was arrested soon after. Further investigative work identified Zazi's co-conspirators and located bomb-making components related to the planned attack. Zazi and one of his confederates later pled guilty and cooperated with the government, while another confederate was convicted and sentenced to life imprisonment. Without the initial tip-off about Zazi and his plans, which came about by monitoring an overseas foreigner under Section 702, the subway-bombing plot might have succeeded.

In cases like the Zazi and Ouazzani investigations, one might ask whether the government could have monitored the communications of the overseas extremists without Section 702, using the traditional FISA process. In some instances, that might be the case. But the process of obtaining court approval for the surveillance under the standards of traditional FISA may, for the reasons explained above, limit the number of people the government can feasibly target and increase the delay before surveillance on a target begins, such that significant communications could be missed.

The Board has received information about other instances in which the Section 702 program has played a role in counterterrorism efforts. Most of these instances are included in a compilation of 54 "success stories" involving the Section 215 and 702 programs that was prepared by the Intelligence Community last year in the wake of Edward Snowden's unauthorized disclosures. Other examples have been shared with the Board more recently. Information about these cases has not been declassified, but some general information about them can be shared. In approximately twenty cases that we have reviewed, surveillance conducted under Section 702 was used in support of an already existing counterterrorism investigation, while in approximately thirty cases, Section 702

information was the initial catalyst that identified previously unknown terrorist operatives and/or plots. In the vast majority of these cases, efforts undertaken with the support of Section 702 appear to have begun with narrowly focused surveillance of a specific individual whom the government had a reasonable basis to believe was involved with terrorist activities, leading to the discovery of a specific plot, after which a short, intensive period of further investigation ensued, leading to the identification of confederates and arrests of the plotters. A rough count of these cases identifies well over one hundred arrests on terrorism-related offenses. In other cases that did not lead to disruption of a plot or apprehension of conspirators, Section 702 appears to have been used to provide warnings about a continuing threat or to assist in investigations that remain ongoing. Approximately fifteen of the cases we reviewed involved some connection to the United States, such as the site of a planned attack or the location of operatives, while approximately forty cases exclusively involved operatives and plots in foreign countries.[472]

C. Contributions to Other Foreign Intelligence Efforts

As noted above, the oversight mandate of our Board extends only to those measures taken by the government to protect the nation from terrorism. Some governmental activities, including the Section 702 program, are not aimed exclusively at preventing terrorism but also serve other foreign intelligence and foreign policy goals. The Section 702 program, for instance, is also used for surveillance aimed at countering the efforts of proliferators of weapons of mass destruction.[473] Given that these other foreign intelligence purposes of the program are not strictly within the Board's mandate, we have not scrutinized the effectiveness of Section 702 in contributing to those other purposes with the same rigor that we have applied in assessing the program's contribution to counterterrorism. Nevertheless, we have come to learn how the program is used for these other purposes, including, for example, specific ways in which it has been used to combat weapons proliferation and the degree to which the program supports the government's efforts to gather foreign intelligence for the benefit of policymakers. Our assessment is that the program is highly valuable for these other purposes, in addition to its usefulness in supporting efforts to prevent terrorism.

---

472 The examples described in this paragraph do not represent an exhaustive list of all instances in which the Section 702 program has proven useful, even in counterterrorism efforts.

473 *See* S. Rep. No. 112-229, at 32 (2012) (appendix reproducing Background Paper on Title VII of FISA Prepared by the Department of Justice and the Office of the Director or National Intelligence) ("Section 702 . . . lets us collect information about the intentions and capabilities of weapons proliferators and other foreign adversaries who threaten the United States.").

III. Privacy and Civil Liberties Implications of the Section 702 Program

A. Nature of the Collection under Section 702

1. Programmatic Surveillance

Unlike the telephone records program conducted by the NSA under Section 215 of the USA PATRIOT Act, the Section 702 program is not based on the indiscriminate collection of information in bulk. Instead, the program consists entirely of targeting specific persons about whom an individualized determination has been made. Once the government concludes that a specific non-U.S. person located outside the United States is likely to communicate certain types of foreign intelligence information — and that this person uses a particular communications "selector," such as an email address or telephone number — the government acquires only those communications involving that particular selector.[474]

Every individual decision to target a particular person and acquire the communications associated with that person must be documented and approved by senior analysts within the NSA before targeting. Each targeting decision is later reviewed by an oversight team from the DOJ and the ODNI ("the DOJ/ODNI oversight team") in an effort to ensure that the person targeted is reasonably believed to be a non-U.S. person located abroad, and that the targeting has a legitimate foreign intelligence purpose. The FISA court does not approve individual targeting decisions or review them after they are made.

Although the "persons" who may be targeted under Section 702 include corporations, associations, and entities as well as individuals,[475] the government is not exploiting any legal ambiguity by "targeting" an entity like a major international terrorist organization and then engaging in indiscriminate or bulk collection of communications in order to later identify a smaller subset of communications that pertain to the targeted entity. To put it another way, the government is not collecting wide swaths of communications and then combing through them for those that are relevant to terrorism or contain other foreign intelligence. Rather, the government first identifies a communications identifier, like an email address, that it reasonably believes is used by the target, whether that target is an individual or an entity. It then acquires only those communications that are related to this identifier.[476] In other words, selectors are always

---

474 See pages 20-23 and 32-33 of this Report.

475 *See* 50 U.S.C. §§ 1801(m), 1881a(a).

476 The NSA's "upstream collection" (described elsewhere in this Report) may require access to a larger body of international communications than those that contain a tasked selector. Nevertheless, the government has no ability to examine or otherwise make use of this larger body of communications, except to promptly determine whether any of them contain a tasked selector. Only those communications (or more precisely, "transactions") that contain a tasked selector go into government databases. See pages 36-41 of this Report.

For now, therefore, "about" collection is an inextricable part of the NSA's upstream collection, which we agree has unique value overall that militates against eliminating it entirely. As a result, any policy debate about whether "about" collection should be eliminated in whole or in part may be, to some degree, a fruitless exercise under present conditions. From our perspective, given a choice between the status quo and crippling upstream collection as a whole, we believe the status quo is reasonable. As explained later, however, because of the serious and novel questions raised by "about" collection as a constitutional and policy matter, we recommend that the NSA develop technology that would allow it to selectively limit or segregate certain forms of "about" communications — so that a debate can be had in which the national security benefits of the different forms of "about" collection are weighed against their respective privacy implications.

We emphasize, however, that our acceptance of "about" collection rests on the considerations described above — the inextricability of the practice from a broader form of collection that has unique value, and the limited nature of what "about" collection presently consists of: the acquisition of Internet communications that include the communications identifier of a targeted person. Although those identifiers may sometimes be found in the body of a communication, the government is not making any effort to obtain communications based on the ideas expressed therein. We are not condoning expanding "about" collection to encompass names or key words, nor to its use in PRISM collection, where it is not similarly inevitable. Finally, our unwillingness to call for the end of "about" collection is also influenced by the constraints that presently govern the use of such communications after acquisition. As with all upstream collection, "about" communications have a default retention period of two years instead of five, are not routed to the CIA or FBI, and may not be queried using U.S. person identifiers.

4. Multi-Communication Transactions ("MCTs")

The technical means used to conduct the NSA's upstream collection result in another issue with privacy implications. Because of the manner in which the agency intercepts communications directly from the Internet "backbone," the NSA sometimes acquires communications that are not themselves authorized for collection (because they are not to, from, or "about" a tasked selector) in the process of acquiring a communication that *is* authorized for collection (because it is to, from, or "about" a tasked selector). In 2011, the FISA court held that the NSA's procedures for addressing this problem were inadequate, and that without adequate procedures this aspect of the NSA's collection practices violated the Fourth Amendment. The government subsequently altered its procedures to the satisfaction of the FISA court. Based on the Board's assessment of how those procedures are being implemented today, the Board agrees that existing practices strike a reasonable balance between national security and privacy.

EXHIBIT D

LIBERTY AND SECURITY IN A CHANGING WORLD

12 December 2013

Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies

This page has been intentionally left blank.

Transmittal Letter

Dear Mr. President:

We are honored to present you with the Final Report of the Review Group on Intelligence and Communications Technologies. Consistent with your memorandum of August 27, 2013, our recommendations are designed to protect our national security and advance our foreign policy while also respecting our longstanding commitment to privacy and civil liberties, recognizing our need to maintain the public trust (including the trust of our friends and allies abroad), and reducing the risk of unauthorized disclosures.

We have emphasized the need to develop principles designed to create strong foundations for the future. Although we have explored past and current practices, and while that exploration has informed our recommendations, this Report should not be taken as a general review of, or as an attempt to provide a detailed assessment of, those practices. Nor have we generally engaged budgetary questions (although some of our recommendations would have budgetary implications).

We recognize that our forty-six recommendations, developed over a relatively short period of time, will require careful assessment by a wide range of relevant officials, with close reference to the likely consequences. Our goal has been to establish broad understandings and principles that

can provide helpful orientation during the coming months, years, and decades.

We are hopeful that this Final Report might prove helpful to you, to Congress, to the American people, and to leaders and citizens of diverse nations during continuing explorations of these important questions.

Richard A. Clarke

Michael J. Morell

Geoffrey R. Stone

Cass R. Sunstein

Peter Swire

According to NSA, section 702 "is the most significant tool in NSA collection arsenal for the detection, identification, and disruption of terrorist threats to the US and around the world." To cite just one example, collection under section 702 "was critical to the discovery and disruption" of a planned bomb attack in 2009 against the New York City subway system" and led to the arrest and conviction of Najibullah Zazi and several of his co-conspirators.[145]

According to the Department of Justice and the Office of the Director of National Intelligence in a 2012 report to Congress:

> Section 702 enables the Government to collect information effectively and efficiently about foreign targets overseas and in a manner that protects the privacy and civil liberties of Americans. Through rigorous oversight, the Government is able to evaluate whether changes are needed to the procedures or guidelines, and what other steps may be appropriate to safeguard the privacy of personal information. In addition, the Department of Justice provides the joint assessments and other reports to the FISC. The FISC has been actively involved in the review of section 702 collection. Together, all of these mechanisms ensure thorough and continuous oversight of section 702 activities. . . .
>
> Section 702 is vital to keeping the nation safe. It provides information about the plans and identities of terrorists,

[145] National Security Agency, *The National Security Agency: Missions, Authorities, Oveersight and Partnerships* (August 9, 2013).

> allowing us to glimpse inside terrorist organizations and obtain information about how those groups function and receive support. In addition, it lets us collect information about the intentions and capabilities of weapons proliferators and other foreign adversaries who threaten the United States.[146]

In reauthorizing section 702 for an additional five years in 2012, the Senate Select Committee on Intelligence concluded:

> [T]he authorities provided [under section 702] have greatly increased the government's ability to collect information and act quickly against important foreign intelligence targets. The Committee has also found that [section 702] has been implemented with attention to protecting the privacy and civil liberties of US persons, and has been the subject of extensive oversight by the Executive branch, the FISC, as well as the Congress. . . . [The] failure to reauthorize [section 702] would "result in a loss of significant intelligence and impede the ability of the Intelligence Community to respond quickly to new threats and intelligence opportunities."[147]

Our own review is not inconsistent with this assessment. During the course of our analysis, NSA shared with the Review Group the details of 54

---

[146] Background Paper on Title VII of FISA Prepared by the Department of Justice and the Office of the Director of National Intelligence (ODNI), Appendix to Senate Select Committee on Intelligence, *Report on FAA Sunsets Extension Act of 2012*, 112th Congress, Cong., 2d Session (June 7, 2012).

[147] Senate Select Committee on Intelligence, *Report on FAA Sunsets Extension Act of 2012*, 112th Congress, 2d Session (June 7, 2012).

counterterrorism investigations since 2007 that resulted in the prevention of terrorist attacks in diverse nations and the United States. In all but one of these cases, information obtained under section 702 contributed in some degree to the success of the investigation. Although it is difficult to assess precisely how many of these investigations would have turned out differently without the information learned through section 702, we are persuaded that section 702 does in fact play an important role in the nation's effort to prevent terrorist attacks across the globe.

* * * * * * * * *

Although section 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 (and thus helps protect our allies), the question remains whether it achieves that goal in a way that unnecessarily sacrifices individual privacy and damages foreign relations. Because the effect of section 702 on United States persons is different from its effect on non-United States persons, it is necessary to examine this question separately for each of these categories of persons.

C. Privacy Protections for United States Persons Whose Communications are Intercepted Under Section 702

Recommendation 12

We recommend that, if the government legally intercepts a communication under section 702, or under any other authority that justifies the interception of a communication on the ground that it is directed at a non-United States person who is located outside the United

EXHIBIT E

JOYCE R. BRANDA
Acting Assistant Attorney General
JOSEPH H. HUNT
Director, Federal Programs Branch
ANTHONY J. COPPOLINO
Deputy Branch Director
JAMES J. GILLIGAN
Special Litigation Counsel
MARCIA BERMAN
Senior Trial Counsel
RODNEY PATTON
JULIA BERMAN
Trial Attorneys
U.S. Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Avenue, NW
Washington, D.C. 20001
Phone: (202) 514-2205
Fax: (202) 616-8470
Attorneys for the United States and Government Defendants Sued in their Official Capacities

UNITED STATES DISTRICT COURT
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 **PUBLIC DECLARATION OF JAMES R. CLAPPER, DIRECTOR OF NATIONAL INTELLIGENCE** Hearing: October 31, 2014 The Honorable Jeffrey S. White

1. (U) I am the Director of National Intelligence ("DNI") of the United States, a position I have held since August 9, 2010. In my capacity as the DNI, I oversee the U.S. Intelligence Community and serve as the principal intelligence advisor to the President. I submit this declaration to confirm that the classified facts set forth in the Classified Declaration of Miriam P., National Security Agency ("Classified Miriam P. Declaration") (submitted *ex* parte, *in* camera, concurrent with the filing of this declaration), fall within the scope of my assertion of the state secrets privilege already made in this case. The statements made herein are based on my personal knowledge and on information made available to me as the DNI.

2. (U) I have reviewed the Classified Miriam P. Declaration, which advises the Court of particular operational details of the NSA's "Upstream" collection of communications under Section 702 of the Foreign Intelligence Surveillance Act that are implicated by Plaintiffs' Motion for Partial Summary Judgment (ECF No. 261). I agree with Ms. Miriam P. that, although the Government has publicly released some information about NSA's Upstream collection, the operational details discussed in the Classified Miriam P. Declaration have not been officially disclosed and remain classified.

3. (U) I further agree that the operational details set forth in her declaration fall within my assertion of the state secrets privilege in this case first made in September 2012 and reaffirmed in large part in December 2013. *See* Public Declaration of James R. Clapper, DNI (Sept. 11, 2012) (ECF No. 104) ¶¶ 10.C; Public Declaration of James R. Clapper, DNI (Dec. 20, 2013) (ECF No. 168) ¶¶ 19.C.1.b. These details, if disclosed, would provide our Nation's adversaries, including foreign terrorist organizations, with unparalleled insight into exactly how the Upstream process works, and permit sophisticated adversaries to further refine and advance their capabilities to avoid US government surveillance activities. This is not an academic concern. The Intelligence Community has seen terrorist groups and other foreign intelligence targets adopt or alter their security practices in direct response to public discussions, whether accurate or inaccurate, of the sources and methods U.S. intelligence agencies use to execute their assigned foreign intelligence responsibilities. Therefore, disclosure of specific information regarding Upstream 702 collection, whether for purposes of addressing the allegations in Plaintiffs' partial motion for summary judgment, for litigating the remainder of plaintiff's claims, or for any other purpose, could reasonably be expected to cause exceptionally grave damage to national security.

(U) I declare under penalty of perjury that the foregoing is true and correct.

DATE: September 29, 2014

JAMES R. CLAPPER
Director of National Intelligence

JOYCE R. BRANDA
Acting Assistant Attorney General
JOSEPH H. HUNT
Director, Federal Programs Branch
ANTHONY J. COPPOLINO
Deputy Branch Director
JAMES J. GILLIGAN
Special Litigation Counsel
james.gilligan@usdoj.gov
MARCIA BERMAN
Senior Trial Counsel
marcia.berman@usdoj.gov
RODNEY PATTON
Trial Attorney
JULIA BERMAN
Trial Attorney
U.S. Department of Justice, Civil Division
20 Massachusetts Avenue, NW
Washington, D.C. 20001
Phone: (202) 616-8480; Fax: (202) 616-8470
Attorneys for the Government Defs. in their Official Capacity

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
OAKLAND DIVISION

CAROLYN JEWEL, *et al.*, Plaintiffs, v. NATIONAL SECURITY AGENCY, *et al.*, Defendants.	Case No. 4:08-cv-04373-JSW **PROPOSED ORDER**

The above-captioned case is before the Court on Plaintiffs' Motion for Partial Summary Judgment, ECF No. 261. The Court, having considered the Plaintiffs' motion, the Government Defendants' opposition, and any reply thereto, IT IS HEREBY ORDERED, that Plaintiffs'

motion for partial summary judgment is DENIED.

AND IT IS SO ORDERED.

Dated: _____

_____
JEFFREY S. WHITE
UNITED STATES DISTRICT JUDGE