S. AMANDA MARSHALL, OSB #95347
United States Attorney
District of Oregon
ETHAN D. KNIGHT, OSB #99298
PAMALA R. HOLSINGER, OSB # 89263
Assistant United States Attorneys
ethan.knight@usdoj.gov
pamala.holsinger@usdoj.gov
1000 SW Third Ave., Ste. 600
Portland, OR 97204-2902
Telephone: (503) 727-1000
Facsimile: (503) 727-1117
JOHN P. CARLIN
Assistant Attorney General
for National Security
GEORGE Z. TOSCAS
J. BRADFORD WIEGMANN
TASHINA GAUHAR
Deputy Assistant Attorneys General
National Security Division
JOLIE F. ZIMMERMAN, DCB #465110
Trial Attorney
Counterterrorism Section
National Security Division
United States Department of Justice
Attorneys for United States of America

UNITED STATES DISTRICT COURT

DISTRICT OF OREGON

PORTLAND DIVISION

UNITED STATES OF AMERICA, **Case No. 3:10-cr-00475-KI**

v.

MOHAMED OSMAN MOHAMUD,

Defendant.

GOVERNMENT'S UNCLASSIFIED RESPONSE TO DEFENDANT'S ALTERNATIVE MOTION FOR SUPPRESSION OF EVIDENCE AND A NEW TRIAL

TABLE OF CONTENTS

I. INTRODUCTION

A. OVERVIEW

On April 4, 2014, defendant Mohamed Osman Mohamud ("defendant") filed his Alternative Motion for Suppression of Evidence and a New Trial Based on the Government's Introduction of Evidence at Trial and Other Uses of Information Derived from Unlawful Electronic Surveillance ("Def.'s Supp. Mot.," ECF No. 502), along with a supporting memorandum of law ("Def.'s Supp. Mem.," ECF No. 503). In his motion, defendant seeks: (1) suppression of any evidence obtained through warrantless surveillance used in his case; (2) vacation of his conviction; (3) a new trial; and (4) suppression of all evidence and other derivative uses of alleged unlawful surveillance, including any fruits of any action taken or decisions based on such surveillance. (Def.'s Supp. Mem., p. 52). On January 13, 2014, defendant filed his Motion for Full Discovery Regarding the Facts and Circumstances Underlying Surveillance ("Def.'s Discovery Mot.," ECF No. 488), along with a supporting memorandum of law ("Def.'s Discovery Mem.," ECF No. 489). Defendant's Discovery Motion seeks discovery of records and information relating to, among other things, the legality and conduct of the Section 702 of the FISA Amendments Act of 2008 ("FAA") collection from which certain of the evidence used at defendant's trial was derived, including the applicable procedures (collectively, "the Section 702 materials"). For the reasons set forth below, the Court should deny defendant's motions in their entirety.[1]

Defendant's motions for discovery and suppression were filed in response to the government's Supplemental FISA Notification, filed on November 19, 2013, which provided "notice to defendant and the Court, pursuant to 50 U.S.C. §§ 1806(c) and 1881e(a), that the

[1] **[CLASSIFIED MATERIAL REDACTED]**

government has offered into evidence or otherwise used or disclosed in proceedings, including at trial," in this case "information derived from the acquisition of foreign intelligence information conducted pursuant to the Foreign Intelligence Surveillance Act of 1978 [FISA], as amended, 50 U.S.C. § 1881a." ("Government's Supplemental Notification," ECF No. 486). The Supplemental Notification was filed based on a recent determination by the government that certain evidence referenced in the original FISA notification, filed on November 29, 2010 (ECF No. 4), obtained or derived from Title I and Title III collection, was itself also derived from Title VII collection as to which defendant was aggrieved. Section 702 of the FAA (part of Title VII of FISA and codified at Section 1881a of FISA) permits the targeting of non-U.S. persons reasonably believed to be located outside the United States, in order to acquire foreign intelligence information, subject to certain statutory requirements. *See* 50 U.S.C. § 1881a. Defendant seeks suppression of the Section 702-derived evidence used in this case, as well as the other relief detailed above.

Defendant's motions have triggered this Court's review of the relevant Section 702 materials pursuant to 50 U.S.C. §§ 1806(f) and 1881e(a) to determine whether the Section 702 intelligence collection was lawfully authorized and conducted. In particular, Section 1806(f) provides that, where the Attorney General certifies that "disclosure [of FISA materials] or an adversary hearing would harm the national security of the United States," a district court "shall, notwithstanding any other law … review *in camera* and *ex parte* the application, order, and such other materials relating to the surveillance of the aggrieved person as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted." 50 U.S.C. § 1806(f). This same procedure applies to motions to disclose Section 702-related materials or to suppress information obtained or derived from Section 702

acquisition, which is deemed to be electronic surveillance pursuant to Title I of FISA for purposes of such motions. 50 U.S.C. § 1881e(a). The Attorney General has filed such a declaration in this case. *See* Declaration and Claim of Privilege of the Attorney General of the United States (Exhibit 1).

Once the Attorney General files a declaration, the court "may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance." 50 U.S.C. § 1806(f). As explained below, this Court should conduct an *in camera, ex parte* review of the documents relevant to defendant's motion, in accordance with the provisions of 50 U.S.C. § 1806(f) and § 1881(e)(a). *See also* 50 U.S.C. § 1825(g).

[CLASSIFIED MATERIAL REDACTED]

In opposition to defendant's motion, the government submits this unclassified memorandum of law. In this unclassified version of the classified memorandum, all classified information, and all header, footer, and paragraph classification markings have been redacted.[2]

[CLASSIFIED MATERIAL REDACTED]

B. SUMMARY OF THE ARGUMENT

[CLASSIFIED MATERIAL REDACTED]

1. Section 702 Is Constitutional

In his motion to suppress evidence derived from Section 702 foreign intelligence acquisition, defendant argues that Section 702 of the FAA violates the Fourth Amendment, Article III, and the First Amendment of the United States Constitution. As an initial matter, this

[2] As a result of the redactions, the pagination and footnote numbering of the classified memorandum and the unclassified memorandum are different.

Court's review should be limited to the constitutionality of the statute as applied to the acquisition of the information challenged in this case. *See In re Directives*, 551 F.3d 1004, 1010 (FISC Ct. Rev. 2008) ("Where, as here, a statute has been implemented in a defined context, an inquiring court may only consider the statute's constitutionality in that context; the court may not speculate about the validity of the law as it might be applied in different ways or on different facts"); *United States v. Posey*, 864 F.2d 1487, 1491 (9th Cir. 1989). As applied to the acquisition at issue here, Section 702 is constitutional. *See infra* at Part IV.

First, the Section 702 collection at issue was reasonable under the Fourth Amendment. The collection lawfully targeted non-U.S. person(s) located outside the United States, who generally are not protected by the Fourth Amendment, for foreign intelligence purposes. That U.S. persons' communications might be incidentally acquired during such collection does not trigger a warrant requirement. Nor does that fact render the collection unreasonable, in light of the compelling national security interests at stake and the extensive procedural safeguards that protect the privacy interests of U.S. persons. *See infra* at Part IV.A.3.

Second, Section 702, in requiring the FISC to review the government's proposed certifications and implementing procedures for acquisitions, does not place the FISC in a role inconsistent with that accorded to Article III courts under the Constitution. The FISC's role under Section 702 is similar to the ability of federal courts to review *ex parte* applications for warrants, wiretap orders, and subpoenas. Like those provisions, Section 702 is entirely consistent with governing Article III principles. *See infra* at Part IV.B.

Third, defendant fails to show that Section 702 violates the First Amendment by "chilling" the expressive activities of third parties. (Def.'s Mem., pp. 37-39). Defendant's claim that the statute has an unconstitutional chilling effect on Americans generally and on various

specific third parties does not provide a basis for exclusion of evidence in a criminal case. Additionally, the Supreme Court and Ninth Circuit have held that when the government's investigative activities have an effect on individuals' First Amendment interests, those interests are safeguarded by adherence to Fourth Amendment standards. *See infra* at Part IV.C. Finally, even if defendant's constitutional arguments had merit, the good-faith exception would preclude exclusion of the evidence. *See infra* at Part IV.D.

2. The Collection in This Case Was Lawfully Authorized and Conducted

In addition to challenging the general constitutionality of Section 702, defendant also questions the government's compliance with the applicable procedures with respect to the specific information that has been used in his case. The government submits that this Court's *in camera*, *ex parte* review of the relevant classified materials will establish that the Section 702 acquisition at issue was lawfully authorized and conducted. First, the applicable certifications and procedures, all of which were reviewed and approved by the FISC, complied with all of Section 702's requirements. Second, the Section 702 collection at issue was conducted in accordance with the statute and those approved certifications and procedures. *See infra* at Part V.

[CLASSIFIED MATERIAL REDACTED]

3. Defendant's Motion for Discovery of the Section 702 Materials Should Be Denied

Because the Attorney General has certified that disclosure of the classified FISA materials would harm the national security of the United States, the Court may disclose these materials (or portions thereof) "only where such disclosure is *necessary* to make an accurate determination of the legality of the surveillance [or search]." 50 U.S.C. § 1806(f) (emphasis

added). Here, the government submits that the Court will be able to determine the legality of the Section 702 collection at issue without the need to compel disclosure of classified materials to the defense. As the government's submissions make clear, the Section 702 collection was lawful and the defendant's allegations to the contrary may be considered, and rejected, based on an examination of the classified record. Contrary to defendant's contention, and as this Court's review of the classified record will show, there is no basis for a finding of material misrepresentations or other factors that would indicate a need for disclosure in this case. *See infra* at Part VII.

4. Defendant's Motion to Suppress Evidence Based on the Collection of Telephony Metadata and Other Alleged Surveillance Activities Should Be Rejected

[CLASSIFIED MATERIAL REDACTED]

5. No *Franks* Hearing Should Be Held

Finally, defendant is not entitled to a hearing under *Franks v. Delaware*, 438 U.S. 154 (1978), because of alleged material omissions from the FISA applications that were the subject of the pre-trial litigation. There were no material omissions or misrepresentations of fact. Rather, the relevant information regarding the prior surveillance was made available to the FISC and this Court. Moreover, defendant's reliance on alleged governmental misconduct and misrepresentations in other, unrelated matters cannot establish a *Franks* violation in this case. There is no basis on which to hold a *Franks* hearing.

[CLASSIFIED MATERIAL REDACTED]

II. BACKGROUND

A. THE FBI'S INVESTIGATION OF DEFENDANT

[CLASSIFIED MATERIAL REDACTED]

B. PROCEDURAL HISTORY

On November 26, 2010, defendant was arrested on a criminal complaint filed in the District of Oregon charging him with attempted use of a weapon of mass destruction, in violation of 18 U.S.C. § 2332a(a)(2)(A). He was indicted on November 29, 2010, by a Portland federal grand jury on the same charge. On November 29, 2010, the government notified this Court and defendant, pursuant to 50 U.S.C. §§ 1806(c) and 1825(d), that the government intended to introduce at trial or otherwise use against defendant information obtained and derived from electronic surveillance and physical searches conducted pursuant to FISA Titles I and III, 50 U.S.C. §§ 1801-1812 and 1821-1829. On June 22, 2011, defendant filed his Motion for Disclosure of FISA-Related Material Necessary to Litigate Motions for Discovery and for Suppression of the Fruits of FISA Activity (ECF No. 54), along with a supporting memorandum of law (ECF No. 55). The government filed its response to defendant's motion on March 8, 2012 ("FISA Suppression Motion Response," ECF No. 81). On May 7, 2012, this Court denied defendant's motion. (Opinion and Order, May 7, 2012, ECF No. 126). On January 31, 2013, defendant was found guilty of attempting to use a weapon of mass destruction after a 13-day jury trial.

On November 19, 2013, the government filed the Supplemental Notification. (ECF No. 486). On January 13, 2014, defendant filed his motion for discovery of Section 702 materials (ECF No. 488). On April 4, 2014, defendant filed the instant motion to suppress (ECF No. 502). Oral argument on defendant's motions has been set for June 4, 2014.

C. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

/ / /

1. Section 702-Acquired Communications

[CLASSIFIED MATERIAL REDACTED]

In the memorandum filed in support of defendant's Motion for Vacation of Conviction and Alternative Remedies of Dismissal of the Indictment, Suppression of Evidence, and New Trial for the Government's Violation of the Pretrial Notice Statute (ECF No. 501) (Def.'s New Trial Mem.), defendant suggests that the Court "determine if the communication[s] introduced at trial or otherwise used is the same as the communication[s] acquired by the § 702 warrantless surveillance." (Def.'s New Trial Mem., p. 14). Defendant seems to believe that, if this were the case, the government's Supplemental Notification and its expressed reasons for why the notice of the use of Section 702-derived information was delayed would be rendered misleading. (*Id.*).

[CLASSIFIED MATERIAL REDACTED]

2. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

III. OVERVIEW OF FISA AND THE FISA AMENDMENTS ACT

A. THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

Since the founding of this country, the government has relied on foreign intelligence collection to protect the nation. For the majority of that time and through the present day, much of this intelligence gathering has been conducted under the President's constitutional authority over national security and foreign affairs, with methods of surveillance evolving over time in light of developing technologies. Presidents have authorized warrantless wiretaps for foreign intelligence purposes since at least 1940. *See, e.g.*, *United States v. United States Dist. Court*, 444 F.2d 651, 669-71 (6th Cir. 1971) (reproducing as an appendix memoranda from Presidents Roosevelt, Truman, and Johnson).

In 1978, Congress enacted FISA "to regulate the use of electronic surveillance within the United States for foreign intelligence purposes." *See* S. Rep. No. 95-604, at 7 (1977). The statute was a response to congressional investigations into abuses of surveillance directed at specific American citizens and political organizations. *Id.* at 7-8. FISA was designed to provide a check against such abuses by placing certain types of foreign intelligence surveillance under the oversight of the FISC.

Before the United States may conduct "electronic surveillance," as defined in FISA, to obtain foreign intelligence information, the statute generally requires the government to obtain an order from a judge on the FISC. *See* 50 U.S.C. §§ 1805, 1809(a)(1); *see* 50 U.S.C. §§ 1803(a), 1804(a). To obtain such an order, the government must establish, *inter alia*, probable cause to believe that the "target of the electronic surveillance is a foreign power or an agent of a foreign power" and that "each of the facilities or places at which the surveillance is directed" (inside or outside the United States) "is being used, or is about to be used, by a foreign power or an agent of a foreign power." 50 U.S.C. § 1805(a)(2). The government must also establish that the "minimization procedures" that it will employ are reasonably designed in light of the purpose and technique of the particular surveillance to minimize the acquisition and retention, and prohibit the dissemination, of nonpublic information concerning unconsenting "United States persons," consistent with the government's need to obtain, produce, and disseminate foreign intelligence information. *See* 50 U.S.C. §§ 1801(h), 1805(a)(3) and (c)(2)(A).

In FISA, Congress limited the definition of the "electronic surveillance" governed by the statute to four discrete types of domestically-focused foreign intelligence collection activities. *See* 50 U.S.C. § 1801(f). Specifically, Congress defined "electronic surveillance" to mean (1) the acquisition of the contents of a wire or radio communication obtained by "intentionally

targeting" a "particular, known United States person who is *in the United States*" in certain circumstances; (2) the acquisition of the contents of a wire communication to or from a "person *in the United States*" when the "acquisition occurs in the United States"; (3) the intentional acquisition of the contents of certain radio communications when the "sender and all intended recipients are located *within the United States*"; and (4) the installation or use of a surveillance device "*in the United States*" for monitoring or to acquire information other than from a wire or radio communication in certain circumstances. *Id.* (emphasis added); *cf.* 50 U.S.C. § 1801(i) (defining "United States person" to mean, as to natural persons, a citizen or permanent resident of the United States).

Because of FISA's definition of "electronic surveillance," FISA as originally enacted did not apply to the vast majority of surveillance the government conducted outside the United States. This was true even if that surveillance might specifically target U.S. persons abroad or incidentally acquire, while targeting third parties abroad, communications to or from U.S. persons or persons located in the United States. *See* S. Rep. No. 95-701, 2d Sess. 7 & n.2, 34-35 & n.16 (1978).[3] Congress was told in the hearing leading to FISA's enactment that the acquisition of international communications at the time did not rely on the four types of "electronic surveillance" covered by the definitions in the proposed legislation – including wire interceptions executed in the United States – and thus those operations would not be affected by

[3] Executive Order No. 12,333, as amended, addresses, *inter alia*, the government's "human and technical collection techniques . . . undertaken abroad." Exec. Order No. 12,333, § 2.2, 3 C.F.R. 210 (1981 Comp.), *reprinted as amended in* 50 U.S.C. § 401 note (Supp. II 2008). That Executive Order governs the intelligence community, *inter alia*, in collecting "foreign intelligence and counter-intelligence" abroad, collecting "signals intelligence information and data" abroad, and utilizing intelligence relationships with "intelligence or security services of foreign governments" that independently collect intelligence information. *Id.* §§ 1.3(b)(4), 1.7(a)(1), (5) and (c)(1).

FISA. *See Foreign Intelligence Surveillance Act: Hearing before the Subcomm. On Crim. Laws and Procedures of the S. Judiciary Comm.*, 94th Cong., 2d Sess., at 11 (Mar. 29, 1976 *et seq.*) ("Mar. 29, 1976 FISA Hrg.").[4] Congress heard similar testimony from other witnesses.[5] Accordingly, at the time FISA was enacted, Congress understood that most foreign-to-foreign and international communications fell outside the definition of "electronic surveillance." *See* S. Rep. No. 95-701, at 71 (1978) ("[T]he legislation does not deal with international signals intelligence activities as currently engaged in by the National Security Agency."). Where the government did not intentionally target a particular, known U.S. person in the United States, FISA allowed the government to monitor international communications through radio surveillance, or wire surveillance of transoceanic cables offshore or on foreign soil, outside the statute's regulatory framework.

/ / /

/ / /

---

[4] Attorney General Levi subsequently elaborated: "The bill does not purport to cover interceptions of all international communications where, for example, the interception would be accomplished outside of the United States, or, to take another example, a radio transmission that does not have both the sender and all intended recipients within the United States." *Electronic Surveillance within the United States for Foreign Intelligence Purposes: Hearings before the Subcomm. On Intel. And the Rights of Americans of the S. Select Comm. On Intel.*, 94th Cong., 2d Sess., at 180-81 (Jun. 29, 1976 *et seq.).*

[5] *See, e.g., Foreign Intelligence Surveillance Act: Hearings before the Subcomm. On Courts, Civil Liberties, and the Admin. Of Justice of the H. Comm. On the Judiciary*, 94th Cong., 2d Sess. at 8 (Apr. 12, 1976 *et seq.*) (statement of former Justice Department official Philip Lacovara) ("[N]ot covered [under the bill] are international wire communications since it is relatively simple, I understand, to intercept these communications at a point outside the United States. Similarly, * * * the bill would have no application whatsoever to international radio traffic."); Mar. 29, 1976 FISA Hrg. At 31 testimony of Morton Halperin) (stating that "if I am an American citizen [in the United States] and I make a phone call to London, and the Government picks it up on a transatlantic cable under the ocean, it is not covered," and "if it goes by microwave, or if it passes through Canada, it would not be covered").

B. THE PROTECT AMERICA ACT AND THE FISA AMENDMENTS ACT OF 2008

In 2006, Congress began considering proposed amendments to FISA aimed at modernizing the statute in response to changes in communications technology since its original enactment. *See Modernization of the Foreign Intelligence Surveillance Act: Hearing before the H. Permanent Select Comm. On Intel.,* 109th Cong., 2d Sess. (Jul. 19, 2006). Congress took up the issue concurrently with an inquiry into the Terrorist Surveillance Program ("TSP") – a program authorized by the President after the terrorist attacks of September 11, 2001, which allowed the NSA to intercept communications into, and out of, the United States where the government reasonably believed that a communicant included a member or agent of al Qaeda or an affiliated terrorist organization. S. Rep. No. 110-209 (2007), at 2-5. The TSP was not carried out under FISA or with the authorization of the FISC. The President's confirmation of the program in 2005 led Congress to "inquire vigorously" into the TSP and to "carefully review[] the impact of technological change on FISA collection to assess whether amendments to FISA should be enacted." *Id.* at 2.

///

///

///

///

///

///

///

///

The Director of National Intelligence ("DNI") and other government officials explained the need for this legislation in various appearances before Congress from 2006 to 2008. As the DNI explained, it was necessary to amend FISA because its definition of "electronic surveillance" was "tie[d] to a snapshot of outdated technology." *Modernization of the Foreign Intelligence Surveillance Act: Hearing before the S. Select Comm. on Intel.*, 110th Cong., 1st Sess. (May 1, 2007) ("May 1, 2007 FISA Modernization Hrg."), at 19. The DNI explained further that, since the creation of the definition three decades previously, "[c]ommunications technology ha[d] evolved in ways that have had unforeseen consequences under [the statute]." *Id.*

More specifically, the DNI explained that, whereas international communications were predominantly carried by radio when FISA was enacted, that was no longer true: "Communications that, in 1978, would have been transmitted via radio or satellite, are now transmitted principally by fiber optic cables" – and therefore qualify as wire communications under FISA. *Id.* Thus, many international communications that would have been generally excluded from FISA regulation in 1978, when they were carried by radio, were now potentially included, due merely to a change in technology rather than any intentional decision by Congress. *Id.*[6]

Further, the DNI stated, with respect to the collection of wire communications, FISA's "electronic surveillance" definition "places a premium on the location of the collection." May 1, 2007 FISA Modernization Hrg. at 19; *see* 50 U.S.C. § 1801(f)(2). The DNI explained that technological advances had rendered this distinction outmoded as well: "Legislators in 1978

[6] *Compare* 50 U.S.C. § 1801(f)(2) (defining wire communication as "electronic surveillance" if, *inter alia*, one party is in the United States) *with* 50 U.S.C. § 1801(f)(3) (defining radio communication as "electronic surveillance" only if the sender and all intended recipients are in the United States).

could not have been expected to predict an integrated global communications grid that makes geography an increasingly irrelevant factor. Today, a single communication can transit the world even if the two people communicating are only located a few miles apart." May 1, 2007 FISA Modernization Hrg. at 19. In this environment, regulating communications differently based on the location of collection arbitrarily limits the government's intelligence-gathering capabilities. As the Director of the NSA elaborated in an earlier hearing:

> [As a communication travels the global communications network,] NSA may have multiple opportunities to intercept it as it moves and changes medium. As long as a communication is otherwise lawfully targeted, we should be indifferent to where the intercept is achieved. Signals intelligence is a difficult art and science, especially in today's telecommunication universe. Intercept of a particular communication * * * is always probabilistic, not deterministic. No coverage is guaranteed. We need to be able to use all the technological tools we have.

FISA for the 21st Century: Hearing before the S. Comm. On the Judiciary, 109th Cong., 2d Sess. (Jul. 26, 2006) (statement of then-NSA Director General Michael V. Hayden).

Although FISA was originally crafted to accommodate the government's collection of foreign and international communications as those operations were commonly conducted in 1978, the government in 2008 faced a different communications technology environment and a different terrorist threat and needed greater flexibility than the statute's terms allowed.[7] The fix

[7] As the DNI testified:

> In today's threat environment, ... FISA * * * is not agile enough to handle the community's and the country's intelligence needs. Enacted nearly 30 years ago, it has not kept pace with 21st century developments in communications technology. As a result, FISA frequently requires judicial authorization to collect the communications of non-U.S. – that is foreign – p[ersons] located outside the United States * * * This clogs FISA process with matters that have little to do with protecting civil liberties or privacy of persons in the United States. Modernizing FISA would greatly improve that process and relieve the massive amounts of analytic resources currently being used to craft FISA applications.

needed for this problem, as a Department of Justice official put it, was a "technology-neutral" framework for surveillance of foreign targets – focused not on "how a communication travels or where it is intercepted," but instead on "who is the subject of the surveillance, which really is the critical issue for civil liberties purposes." May 1, 2007 FISA Modernization Hrg. at 46 (statement of Asst. Att'y Gen. Kenneth L. Wainstein).

That review initially led to the enactment in August 2007 of the Protect America Act ("PAA"), Pub. L. 110-55 (2007). Congress enacted the PAA in order to bring FISA "up to date with the changes in communications technology," while at the same time preserving "the privacy interests of persons in the United States" and addressing the "degraded capabilities in the face of a heightened terrorist threat environment" that resulted from FISA's "requirement of a court order to collect foreign intelligence about foreign targets located overseas." S. Rep. No. 110-209, at 5-6 (2007). The PAA fulfilled these purposes by empowering the DNI and the Attorney General to jointly authorize "the acquisition of foreign intelligence information concerning persons reasonably believed to be located outside the United States." 50 U.S.C. § 1805b(a). To authorize such collection, the PAA required the DNI and the Attorney General to certify, *inter alia*, that there were reasonable procedures in place for determining that the acquisition concerned persons (whether U.S. persons or non-U.S. persons) reasonably believed to be located outside the United States ("targeting procedures"), there were minimization procedures in place that satisfied FISA's requirements for such procedures, and a significant purpose of the acquisition was to acquire foreign intelligence information. *See* 50 U.S.C. § 1805b(a)(1)-(5). The PAA also authorized the FISC to review the DNI and Attorney General's determination regarding the reasonableness of the targeting procedures. Finally, the PAA authorized private

---

May 1, 2007 FISA Modernization Hrg. at 18.

parties who had been directed by the government to assist in effectuating surveillance under the statute to challenge the legality of such a directive in the FISC, 50 U.S.C. § 1805b(h)(1)(A), and to appeal an adverse decision to the Foreign Intelligence Surveillance Court of Review ("FISA Court of Review"), *id.* § 1805b(i).[8] One private party brought such a challenge, and both the FISC and the FISA Court of Review upheld the PAA. *See In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act*, 551 F.3d 1004 (FISC Ct. Rev. 2008) (holding that surveillance authorized under the PAA fell within the foreign intelligence exception to the warrant requirement and was otherwise reasonable under the Fourth Amendment).

C. SECTION 702 OF THE FAA

Due to a sunset provision, the PAA expired in February 2008. In July 2008, Congress enacted the FISA Amendments Act of 2008 ("FAA"), Pub. L. No. 110-261, § 101(a)(2), 122 Stat. 2436.[9] The FAA provision at issue here, Section 702 of the FAA (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).[10] Section 702 provides that, "upon the issuance" of an order from the FISC, the Attorney General and DNI may jointly authorize the "targeting of persons reasonably believed to

/ / /

---

[8] The FISA Court of Review is composed of three United States District or Circuit Judges who are designated by the Chief Justice of the Supreme Court. *See* 50 U.S.C. § 1803(b).

[9] In 2012, Congress reauthorized the FAA for an additional five years. *See* FISA Amendments Act Reauthorization Act of 2012, Pub. L. No. 112-238, 126 Stat. 1631.

[10] The FAA enacted other amendments to FISA, including provisions not at issue in this case that govern the targeting of United States persons outside the United States. *See* 50 U.S.C. §§ 1881b, 1881c.

be located outside the United States" for a period of up to one year to acquire "foreign intelligence information." 50 U.S.C. § 1881a(a).[11]

Under Section 1881a(b), the authorized acquisition must comply with each of the following requirements, which are directed at preventing the intentional targeting of U.S. persons or persons located within the United States, or collection of communications known at the time of acquisition to be purely domestic:

> (1) The authorized acquisition "may not intentionally target any person known at the time of acquisition to be located in the United States." 50 U.S.C. § 1881a(b)(1).
>
> (2) It may not intentionally target a person outside the United States "if the purpose . . . is to target a particular, known person reasonably believed to be in the United States." 50 U.S.C. § 1881a(b)(2).
>
> (3) It "may not intentionally target a United States person reasonably believed to be located outside the United States." 50 U.S.C. § 1881a(b)(3).
>
> (4) It may not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States. 50 U.S.C. § 1881a(b)(4).
>
> (5) The acquisition must be "conducted in a manner consistent with the [F]ourth [A]mendment." 50 U.S.C. § 1881a(b)(5).

Section 702 does not require an individualized court order addressing each non-U.S. person to be targeted under its provisions. Section 702 instead permits the FISC to approve annual certifications by the Attorney General and DNI that authorize the acquisition of certain categories of foreign intelligence information through the targeting of non-U.S. persons reasonably believed to be located outside the United States.

---

[11] The Attorney General and DNI may authorize targeting to commence under Section 702 before the FISC issues its order if they determine that certain "exigent circumstances" exist. 50 U.S.C. § 1881a(a), (c)(2). If that determination is made, the Attorney General and DNI must, as soon as practicable (and within seven days), submit for FISC review their Section 702 certification, including the targeting and minimization procedures used in the acquisition. 50 U.S.C. 1881a(g)(1)(B); *see* 50 U.S.C. § 1881a(d), (e), (g)(2)(B).

1. The Government's Submission to the FISC

Section 702 requires the government to obtain the FISC's approval of (1) the government's certification regarding the proposed collection, and (2) the targeting and minimization procedures to be used in the acquisition. 50 U.S.C. § 1881a(a), (c)(1), (i)(2), (3); *see* 50 U.S.C. § 1881a(d), (e), (g)(2)(B). The certification must be made by the Attorney General and DNI and must attest that

> (1) there are targeting procedures in place, that have been or will be submitted for approval by the FISC, that are reasonably designed to ensure that the 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;
>
> (2) the minimization procedures meet the definition of minimization procedures set forth in Titles I and III of FISA (50 U.S.C. §§ 1801(h), 1821(4)) and have been or will be submitted for approval by the FISC;
>
> (3) guidelines have been adopted by the Attorney General to ensure compliance with the aforementioned limitations set forth in Section 1881a(b) prohibiting, among other things, the targeting of United States persons;
>
> (4) the targeting and minimization procedures and guidelines are consistent with the Fourth Amendment;
>
> (5) a significant purpose of the acquisition is to obtain foreign intelligence information;
>
> (6) the acquisition involves obtaining "foreign intelligence information from or with the assistance of an electronic communication service provider"; and
>
> (7) the acquisition complies with the limitations in Section 1881a(b).[12]

50 U.S.C. § 1881a(g)(2)(A)(i) - (vii); *see* 50 U.S.C. §§ 1801(h), 1821(4), 1881a(b); *cf.* 50 U.S.C. §§ 1801(e), 1881(a) (defining "foreign intelligence information"). Such certifications are "not

[12] Those limitations, as described above, generally prevent the intentional targeting of United States persons or persons located within the United States or collection of communications known at the time of acquisition to be purely domestic.

required to identify the specific facilities, places, premises, or property at which an acquisition authorized under [section 1881a(a)] will be directed or conducted." 50 U.S.C. § 1881a(g)(4).[13]

The certification must include copies of the targeting and minimization procedures, and a supporting affidavit, "as appropriate," from the head of an Intelligence Community element or other Senate-confirmed official "in the area of national security." 50 U.S.C. § 1881a(g)(2)(B) - (C). Finally, the certification must include "an effective date for the authorization that is at least 30 days after the submission of the written certification" to the FISC. 50 U.S.C. § 1881a(g)(2)(D)(i).

[CLASSIFIED MATERIAL REDACTED]

2. The FISC's Order

The FISC must review the certification, targeting and minimization procedures, and any amendments thereto. 50 U.S.C. § 1881a(i)(1) and (2). If the FISC determines that the certification contains all the required elements and concludes that the targeting and minimization procedures and Attorney General guidelines for compliance with the statutory limitations are "consistent with" both the Act and "the [F]ourth [A]mendment," the FISC will issue an order approving the certification and the use of the targeting and minimization procedures. 50 U.S.C. § 1881a(i)(3)(A). If the FISC finds deficiencies in the certification or procedures, it must issue an order directing the government to, at the government's election and to the extent required by the court's order, correct any deficiency within 30 days, or cease or not begin implementation of the authorization. 50 U.S.C. § 1881a(i)(3)(B).

[CLASSIFIED MATERIAL REDACTED]

---

[13] **[CLASSIFIED MATERIAL REDACTED]**

3. Implementation of Section 702 Authority

The government acquires communications pursuant to Section 702 through compelled assistance from electronic communications service providers. 50 U.S.C. § 1881a(h). The government identifies to these service providers specific accounts, addresses, and/or identifiers, such as email addresses and telephone numbers, that the government has assessed, through the application of FISC-approved targeting procedures, are likely to be used by non-U.S. persons reasonably believed to be located overseas who possess, communicate, or are likely to receive a type of foreign intelligence information authorized for collection under a certification approved by the FISC. *See* NSA, The National Security Agency: Missions Authorities, Oversight and Partnerships 4 (Aug. 9, 2013) (describing the NSA's collection of foreign intelligence information under Section 702). Such "identifiers are used to select communications for acquisition," and the "[s]ervice providers are compelled to assist [the government] in acquiring the communications associated with those identifiers." *Id.*[14]

[CLASSIFIED MATERIAL REDACTED]

4. Targeting and Minimization Procedures

The government may conduct acquisitions under Section 702 only in accordance with specific targeting and minimization procedures that are subject to review and approval by the FISC. 50 U.S.C. § 1881a(c)(1)(A), (d), (e), and (i)(3)(A). Not only must the targeting procedures be reasonably designed to restrict acquisitions to the targeting of persons reasonably believed to be outside the United States and applied using compliance guidelines to ensure that the acquisitions do not intentionally target U.S. persons or persons located in the United States, 50 U.S.C. §§ 1881a(b), (d)(1) and (f)(1)(A), the minimization procedures also must be

[14] **[CLASSIFIED MATERIAL REDACTED]**

reasonably designed to minimize any acquisition of nonpublicly available information about unconsenting U.S. persons, and to minimize the retention and prohibit the dissemination of any such information that might still be acquired, consistent with the need to obtain, produce, and disseminate foreign-intelligence information. 50 U.S.C. §§ 1801(h)(1), 1821(4)(A); *see* 50 U.S.C. § 1881a(e)(1).[15] The FISC, in turn, must substantively review the targeting and minimization procedures to ensure that they satisfy the statutory criteria and are consistent with the Fourth Amendment. 50 U.S.C. § 1881a(i)(2)(B), (C) and (3)(A).

[CLASSIFIED MATERIAL REDACTED]

a. Targeting Procedures

[CLASSIFIED MATERIAL REDACTED]

b. **[CLASSIFIED MATERIAL REDACTED]**

[CLASSIFIED MATERIAL REDACTED]

c. **[CLASSIFIED MATERIAL REDACTED]**

[CLASSIFIED MATERIAL REDACTED]

d. Minimization Procedures

As noted above, Section 702 also requires the adoption of minimization procedures that comply with FISA's definition of such procedures. *See* 50 U.S.C. § 1881a(e)(1). FISA-compliant minimization procedures are, in pertinent part:

> (1) specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular

[15] Minimization procedures may also "allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes." 50 U.S.C. § 1801(h)(3). The definitions of minimization procedures in 50 U.S.C. §§ 1801(h)(4) and 1821(4)(D), which apply only to electronic surveillance approved pursuant to 50 U.S.C. § 1802(a) and physical searches approved pursuant to 50 U.S.C. § 1822(a), respectively, do not apply to acquisitions conducted under Section 702.

> surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information;
>
> (2) procedures that require that nonpublicly available information, which is not foreign intelligence information . . . , shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance; [and]
>
> (3) notwithstanding paragraphs (1) and (2), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes.

50 U.S.C. § 1801(h); *see also* 50 U.S.C. § 1821(4); 50 U.S.C. § 1801(e) (defining "foreign intelligence information").

[CLASSIFIED MATERIAL REDACTED]

5. Oversight

Section 702 requires that the Attorney General and DNI periodically assess the government's compliance with both the targeting and minimization procedures and with relevant compliance guidelines, and that they submit those assessments both to the FISC and to Congressional oversight committees. 50 U.S.C. § 1881a(*l*). In addition, not less often than once every six months, the Attorney General must keep the relevant Congressional oversight committees "fully inform[ed]" concerning the implementation of Section 702. 50 U.S.C. § 1881f(a) and (b)(1); *see also Clapper*, 133 S. Ct. at 1144 ("Surveillance under [Section 702] is subject to statutory conditions, judicial authorization, congressional supervision, and compliance with the Fourth Amendment.").[16]

[16] Rule 13(b) of the Rules of Procedures for the FISC requires the government to report, in writing, all instances of non-compliance. FISA Ct. R. of P. 13(b). The government reports Section 702 compliance incidents to the FISC via individual notices and quarterly reports. *See*

6. District Court Review of FISC Orders and Section 702 Collection

The FAA authorizes the use in a criminal prosecution of information obtained or derived from the acquisition of foreign intelligence information under Section 702, provided that advance authorization is obtained from the Attorney General and proper notice is subsequently given to the court and to each aggrieved person against whom the information is to be used. 50 U.S.C. § 1881e(a) provides that information acquired pursuant to Section 702 is "deemed to be" information acquired pursuant to Title I of FISA for, among other things, the purposes of the applicability of the statutory notice requirement and the suppression and discovery provisions of Section 1806.

Under Section 1806(c), the government's notice obligation applies only if the government "intends to enter into evidence or otherwise use or disclose" (2) against an "aggrieved person" (3) in a "trial, hearing or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States" (4) any "information obtained or derived from" (5) an "electronic surveillance [or physical search] of that aggrieved person." 50 U.S.C. § 1806(c); *see* 50 U.S.C. § 1825(d).[17] Where all five criteria are met, the government will notify the defense and the Court (or other authority) in which the information is to be disclosed or used that the government intends to use or disclose such information. The

---

NSA, Civil Liberties and Privacy Office Report on NSA's Implementation of FISA Section 702, Apr. 16, 2014, publicly available at http://icontherecord/tumblr.com, at 3. Depending on the type or severity of compliance incidents, the NSA also may promptly notify the relevant Congressional intelligence committees of an individual compliance matter. *Id.* at 3.

[17] An "aggrieved person" is defined as the target of electronic surveillance or "any other person whose communications or activities were subject to electronic surveillance," 50 U.S.C. § 1801(k), as well as "a person whose premises, property, information, or material is the target of physical search" or "whose premises, property, information, or material was subject to physical search." 50 U.S.C. § 1821(2).

"aggrieved" defendant may then challenge the use of that information in district court on two grounds: (1) that the information was unlawfully acquired; or (2) that the acquisition was not conducted in conformity with an order of authorization or approval. 50 U.S.C. §§ 1806(e) and (f), 1881e(a).[18] In assessing the legality of the collection at issue, the district court, "shall, notwithstanding any other law, if the Attorney General files [as he has filed in this proceeding] an affidavit [or declaration] under oath that disclosure or an adversary hearing would harm the national security of the United States, review in camera and ex parte the application, order, and such other materials relating to the surveillance [or physical search] as may be necessary to determine whether the surveillance [or physical search] of the aggrieved person was lawfully authorized and conducted." 50 U.S.C. §§ 1806(f), 1825(g).

On the filing of the Attorney General's affidavit or declaration, the court "may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance [or physical search] only where such disclosure is necessary to make an accurate determination of the legality of the surveillance [or search]. *Id.* If the district court is able to make an accurate determination of the legality of the surveillance or search based on its *in camera*, *ex parte* review of the materials submitted by the United States, then the court may not order disclosure of any of the FISA or FAA materials to the defense, unless otherwise required by due process. *See id.*

///

///

[18] Separately, any electronic communications service provider the government directs to assist in Section 702 surveillance may challenge the lawfulness of that directive in the FISC. 50 U.S.C. § 1881a(h)(4) and (6); *see also In re Directives*, 551 F.3d at 1004 (adjudicating Fourth Amendment challenge brought by electronic communications service provider to directive issued under the PAA).

IV. DEFENDANT'S CONSTITUTIONAL ARGUMENTS LACK MERIT

Defendant moves for suppression of evidence derived from the acquisition of foreign intelligence information under Section 702 on the ground that Section 702 is unconstitutional. (Def.'s Mem., pp. 13-39). For the reasons set forth below, defendant's motion should be denied.

A. THE ACQUISTION OF FOREIGN INTELLIGENCE INFORMATION UNDER SECTION 702 IS LAWFUL UNDER THE FOURTH AMENDMENT

For the reasons set forth below, the collection at issue in this case, pursuant to Section 702 and the applicable certifications and targeting and minimization procedures, was consistent with the Fourth Amendment.

The Fourth Amendment provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated" and that "no Warrants shall issue, but upon probable cause." "[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." *Nat'l Treas. Employees Union v. Von Raab*, 489 U.S. 656, 665 (1989). The "touchstone" of a 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)).

As explained below, the Section 702-authorized collection at issue in this case, which was conducted pursuant to court-approved procedures reasonably designed to target non-U.S. persons located outside the United States, was reasonable under the Fourth Amendment. First,

the Fourth Amendment generally does not apply to non-U.S. persons abroad, and the fact that collection targeting such persons also incidentally collects communications of U.S. persons does not trigger a warrant requirement or render the collection constitutionally unreasonable. Second, surveillance authorized under Section 702 falls within the well-recognized "foreign intelligence exception" to the warrant requirement because (1) the government's purpose – protecting against terrorist attacks and other external threats – extends "beyond routine law enforcement," and (2) "insisting upon a warrant would materially interfere with the accomplishment of that purpose." *In re Directives*, 551 F.3d 1004, 1010-11 (FISC Ct. Rev. 2008).

Given the inapplicability of the warrant requirement, the challenged collection need only meet the Fourth Amendment's general reasonableness standard. That standard is satisfied here. The government has interests of the utmost importance in obtaining foreign intelligence information under Section 702 to protect national security. In contrast, the privacy interests of U.S. persons in international communications are significantly diminished when those communications have been transmitted to or obtained from non-U.S. persons located outside the United States. Finally, the privacy interests of U.S. persons whose communications are incidentally collected are amply protected by stringent safeguards the government employs in implementing the collection. Those safeguards include (1) targeting procedures that reasonably confine acquisitions to targets who are non-U.S. persons located outside the United States; (2) minimization procedures that serve to limit the acquisition, retention, and dissemination of information about U.S. persons and that closely resemble minimization procedures that have been used for decades in the context of foreign intelligence surveillance to protect the privacy interests of U.S. persons; and (3) guidelines adopted by the Attorney General to ensure compliance with the statutory limits on acquisitions. In light of these and other safeguards

employed by the government, the FISC has repeatedly concluded that acquisition of foreign intelligence information under Section 702 and the applicable targeting and minimization procedures is constitutionally reasonable. This Court should reach the same conclusion.

1. There Is No Judicial Warrant Requirement Applicable to Foreign Intelligence Collection Targeted at Foreign Persons Abroad

a. The Fourth Amendment Generally Does Not Apply to Non–U.S. Persons Abroad

The Supreme Court has held that the Fourth Amendment does not "apply to activities of the United States directed against aliens in foreign territory." *United States v. Verdugo-Urquidez*, 494 U.S. 259, 267 (1990); *see also id.* at 271 (noting that only persons who "have come within the territory of the United States and developed substantial connections" to the country have Fourth Amendment rights). Based on the Fourth Amendment's text, drafting history, and post-ratification history, *id.* at 265-67, as well as its own precedents, *id.* at 268-71, the Supreme Court concluded that the Fourth Amendment was not intended "to restrain the actions of the Federal Government against aliens outside of the United States territory," *id.* at 266. "If there are to be restrictions on searches and seizures which occur incident to such American action," the Court explained, "they must be imposed by the political branches through diplomatic understanding, treaty, or legislation." *Id.* at 275. Because the Fourth Amendment generally does not protect non-U.S. persons outside the United States, at least where such persons lack "substantial connections" to this country, the Fourth Amendment *a fortiori* does not prevent the government from subjecting them to surveillance without a warrant.

Intelligence collection under Section 702 targets non-U.S. persons located outside the United States. Accordingly, under *Verdugo-Urquidez,* the Fourth Amendment generally is inapplicable to persons who are targeted for collection in accordance with the requirements of

the statute.[19] For that reason, to the extent defendant attempts a facial challenge to Section 702, the challenge fails, because the statute has a "plainly legitimate sweep" in its intended application to persons unprotected by the Fourth Amendment. *See Washington State Grange v. Washington State Republican Party*, 552 U.S. 442, 449 (2008) (citation omitted).[20]

b. Incidental Collection of U.S. Person Communications Pursuant to Intelligence Collection Lawfully Targeting Non-U.S. Persons Located Outside the United States Does Not Trigger a Warrant Requirement

Defendant, as a U.S. citizen, was not targeted under Section 702. Nevertheless, he is an "aggrieved person" under FISA because his communications were collected *incidentally* under Section 702, in the course of intelligence collection targeted at one or more non-U.S. persons outside the United States. However, in general, "incidental collections occurring as a result of constitutionally permissible acquisitions do not render those acquisitions unlawful." *In re Directives*, 551 F.3d at 1015; *see also United States v. White*, 401 U.S. 745, 751-53 (1971) (holding that a conversation recorded with the consent of one participant did not violate another participant's Fourth Amendment rights); *United States v. Kahn*, 415 U.S. 143, 156-57 (1974) (upholding interception of communications of a woman that were incidentally collected pursuant to a criminal wiretap order targeting her husband); *United States v. Martin*, 599 F.2d 880, 884-85 (9th Cir. 1979), *overruled on other grounds by United States v. De Bright*, 730 F.2d 1255 (9th Cir. 1984) (en banc); *United States v. Figueroa*, 757 F.2d 466, 472-73 (2d Cir. 1985) (rejecting challenge to Title III on the ground that it allows interception of conversations of unknown third

---

[19] The head of each element of the intelligence community must report annually to the FISC concerning, *inter alia*, how many persons the element targeted under Section 1881a (based on the belief that the persons were located outside the United States) who were later determined to be located inside the United States. *See* 50 U.S.C. § 1881a(*l*)(3)(A)(iii).

[20] In any event, as noted *supra* at Part I.B.1., this Court's review should be limited to the constitutionality of the statute as applied to the acquisition of the information challenged in this case.

parties); *United States v. Butenko*, 494 F.2d 593, 608 (3d Cir. 1974) (upholding the constitutionality of warrantless surveillance for foreign intelligence purposes even though "conversations . . . of American citizens[] will be overheard"); *United States v. Bin Laden*, 126 F. Supp. 2d 264, 280 (S.D.N.Y. 2000) ("[I]ncidental interception of a person's conversations during an otherwise lawful surveillance is not violative of the Fourth Amendment.").

Under these principles, incidental capture of a U.S. person's communications during surveillance that lawfully targets non-U.S. persons abroad does not imply that a judicial warrant or other individualized court order is required for such surveillance to be reasonable under the Fourth Amendment. *See Bin Laden*, 126 F. Supp. 2d at 281 (noting that "the combination of *Verdugo-Urquidez* and the incidental interception cases" would permit surveillance that collects a U.S. person's communications as an incident to warrantless surveillance targeting a non-U.S. person abroad, so long as the United States person is not a "known and contemplated" surveillance target). Thus, surveillance of non-U.S. persons outside the United States pursuant to Section 702, even without a warrant or probable cause, is not rendered unlawful if the surveillance incidentally captures the communications of non-targeted persons in the United States. This conclusion is particularly appropriate here because the privacy interests of U.S. persons whose communications are incidentally collected are specifically protected by minimization procedures, as described *supra* at Part III.C.4.d. *See In re Directives*, 551 F.3d at 1016 (noting that the minimization procedures under the PAA "serve . . . as a means of reducing the impact of incidental intrusions into the privacy of non-targeted United States persons").

Application of a warrant requirement to incidental interception of U.S.- person communications during surveillance targeting non-U.S. persons abroad for foreign intelligence purposes not only would be contrary to case law but also would be impracticable and

inconsistent with decades of foreign-intelligence collection practice. *See In re Terrorist Bombings of U.S. Embassies*, 552 F.3d 157, 169 (2d Cir. 2008) (holding that the warrant requirement does not apply to searches or surveillance of U.S. citizens that occur outside the United States because the original purpose of the Fourth Amendment "was to restrict searches and seizures which might be conducted by the United States in domestic matters"); *United States v. Barona*, 56 F.3d 1087, 1092 n.1 (9th Cir. 1995) (foreign searches have "neither been historically subject to the warrant procedure, nor could they be as a practical matter"); *United States v. Stokes*, 726 F.3d 880, 893 (7th Cir. 2013) (rejecting warrant requirement for extraterritorial searches targeting United States persons and holding such searches "are subject only to the Fourth Amendment's requirement of reasonableness").[21] Before initiating surveillance of a foreign target, the government cannot know the identities of all those with whom the target will communicate, and there will generally be at least some possibility that the target will communicate with a U.S. person. *See Bin Laden*, 126 F. Supp. 2d at 280 ("[T]he government is often not in a position of omniscience regarding who or what a particular surveillance will record."). Imposition of a warrant requirement for any incidental interception of U.S. person communications would effectively require a warrant for all foreign intelligence collection, even though the foreign targets lack Fourth Amendment rights and their communications often involve only other foreigners. Such a rule would unduly restrict the government's intelligence collection against foreign targets and degrade its ability to protect against foreign threats. *See Warrantless Surveillance and The Foreign Intelligence Surveillance Act: The Role of Checks and Balances in Protecting Americans' Privacy Rights (Part II)*

[21] While defendant cites a number of cases recognizing a warrant requirement for electronic surveillance in the domestic context (Def.'s Mem., p. 13), he does not point to any authorities indicating that foreign intelligence surveillance targeting non-United States persons outside the United States must be subject to the warrant procedure.

Hearing Before the H. Judiciary Comm., 110th Cong., 1st Sess. at 8 (2007) (statement of Rep. Forbes) ("To require a court order for every instance in which a foreign target communicates with someone inside the United States is to require a court order for every foreign target, and requiring this would reverse 30 years of established intelligence gathering . . . . The intelligence community cannot possibly know ahead of time who these terrorists will talk to. It needs to have the flexibility to monitor calls that may occur between a foreign terrorist and a person inside the United States.").

c. The Location of the Search Does Not Trigger a Warrant Requirement

Verdugo-Urquidez involved a physical search that was conducted overseas, while collection under Section 702 takes place within the United States. In the context of electronic communications, however, the fact that the communications of a non-U.S. person outside the United States may be collected from within the United States is not the kind of "significant voluntary connection with the United States" that brings that person within the protection of the Fourth Amendment under *Verdugo-Urquidez*. 494 U.S. at 271-72. Otherwise, any foreign person abroad seeking to evade United States surveillance, including al Qaeda terrorists, could claim the protections of the Fourth Amendment merely due to this type of insignificant connection to the United States. That result would be plainly contrary to the Supreme Court's statements in *Verdugo-Urquidez* that the Fourth Amendment was originally intended to protect "the people of the United States" rather than "aliens outside of the United States territory." *Id.* at 266-67. Moreover, when the government collects the communications of a non-U.S. person located abroad, whether the collection takes place in the United States or abroad makes no difference to the person's privacy interests and should not affect the constitutional analysis. When it comes to the content of communications, "the Fourth Amendment protects people, not

places." *United States v. Yonn*, 702 F.2d 1341, 1347 (11th Cir. 1983) (quoting *Katz v. United States*, 389 U.S. 347, 351 (1967)). Accordingly, there is no "constitutional distinction which depends upon the location of the recording apparatus." *Yonn*, 702 F.2d at 1347.

2. The Foreign Intelligence Exception Applies

Even assuming, *arguendo*, that incidental collection of U.S.-person communications under Section 702 is subject to the same constitutional scrutiny as foreign intelligence collection targeting U.S. persons, *cf. [Caption Redacted]*, 2011 WL 10945618, *26 (FISC Oct. 3, 2011) (noting that "[t]here surely are circumstances in which incidental intrusions can be so substantial as to render a search or seizure unreasonable"), the Fourth Amendment does not require a warrant here because such surveillance falls within the well-recognized foreign intelligence exception.

a. The "Special Needs" Doctrine

The touchstone of the Fourth Amendment is reasonableness, which is assessed by balancing the degree to which a search is needed to promote legitimate governmental interests against the search's intrusion on a person's privacy interests. *See United States v. Knights*, 534 U.S. 112, 118-19 (2001). In many contexts, a search or surveillance is impermissible without a warrant or other individualized court order. *See Vernonia School Dist. 47J v. Acton*, 515 U.S. 646, 652-53 (1995) ("Where a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing, this Court has said that reasonableness generally requires the obtaining of a judicial warrant."). But that procedure is by no means inflexibly required. *Maryland v. King*, 133 S. Ct. 1958, 1969 (2013) (The Fourth Amendment "imposes no irreducible requirement" of individualized suspicion.); *see, e.g.*, *United States v. Flores-Montano*, 541 U.S. 149, 153 (2004) (The government has "plenary authority to conduct routine

searches and seizures at the border, without probable cause or a warrant.").

The Supreme Court has recognized exceptions to the Fourth Amendment's warrant requirement "when special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable," *Griffin v. Wisconsin*, 483 U.S. 868, 873 (1987), such as where the governmental need is especially compelling or especially likely to be frustrated by a warrant requirement, where expectations of privacy are diminished, and where alternative safeguards restrain the government within reasonable limits. *See King*, 133 S. Ct. at 1969; *see also, e.g. Griffin*, 483 U.S. at 873-74, (upholding warrantless search of probationer's home); *Vernonia School Dist.*, 515 U.S. at 653 (upholding warrantless drug testing of student-athletes by public school district); *Samson v. California*, 547 U.S. 843, 847 (2006) (upholding suspicionless searches of parolees). In evaluating whether the "special needs" doctrine applies, the Supreme Court has distinguished between searches designed to uncover evidence "of ordinary criminal wrongdoing" and those motivated "at [a] programmatic level" by other governmental objectives. *City of Indianapolis v. Edmond*, 531 U.S. 32, 37-40, 48 (2000) (reviewing cases).

The "special needs" doctrine applies where special government interests beyond the normal need for law enforcement make the warrant and probable-cause requirement impracticable, and in such cases the court "employ[s] a balancing test that weigh[s] the intrusion on the individual's interest in privacy against the 'special needs' that supported the program." *Ferguson v. City of Charleston*, 532 U.S. 67, 78 (2001). Accordingly, the Supreme Court has permitted, *inter alia*, warrantless stops of motorists at roadblocks for the purpose of securing borders, *see United States v. Martinez-Fuerte*, 428 U.S. 543 (1976), warrantless searches of the homes of probationers to ensure compliance with probation conditions, *see Griffin*, 483 U.S. at

872, and warrantless searches of public school students to enforce school rules, *see T.L.O.*, 469 U.S. at 340.

b. The Foreign Intelligence Exception

Several courts of appeals – including the FISA Court of Review – have held, by analogy to the "special needs" doctrine, that the government's "special need" for foreign intelligence information justifies an exception to the warrant requirement. *See, e.g., United States v. Buck*, 548 F.2d 871, 875 (9th Cir. 1977) ("Foreign security wiretaps are a recognized exception to the general warrant requirement."); *United States v. Duka*, 671 F.3d 329, 341 (3d Cir. 2011) ("[C]ourts [that have considered the question] almost uniformly have concluded that the important national interest in foreign intelligence gathering justifies electronic surveillance without prior judicial review, creating a sort of 'foreign intelligence exception' to the Fourth Amendment's warrant requirement."); *In re Directives*, 551 F.3d at 1010-11 (recognizing "a foreign intelligence exception" to the warrant requirement); *In re Sealed Case*, 310 F.3d 717, 742 (FISA Ct. Rev. 2002) ("[A]ll the . . . courts to have decided the issue [have] held that the President did have inherent authority to conduct warrantless searches to obtain foreign intelligence information."); *United States v. Truong Dinh Hung*, 629 F.2d 908, 912-13 (4th Cir. 1980) (upholding warrantless foreign intelligence surveillance authorized by the Attorney General); *Butenko*, 494 F.2d at 605 (upholding warrantless foreign intelligence surveillance); *United States v. Brown*, 484 F.2d 418, 426 (5th Cir. 1973) (holding that "the President may constitutionally authorize warrantless wiretaps for the purpose of gathering foreign intelligence");[22] *but see Zweibon v. Mitchell*, 516 F.2d 594, 618-20 (D.C. Cir. 1975) (en banc)

[22] Except for *In re Directives*, these cases involved collection of foreign intelligence information from persons inside the United States. Their reasoning applies *a fortiori* to the Section 702

(plurality opinion suggesting in dicta that a warrant may be required even in a foreign intelligence investigation).[23] These decisions have found that foreign intelligence collection justifies an exception because the "programmatic purpose" of obtaining foreign intelligence information goes "beyond any garden-variety law enforcement objective," and "requiring a warrant would hinder the government's ability to collect time-sensitive information and, thus, would impede the vital national security interests that are at stake." *In re Directives*, 551 F.3d at 1011.

Contrary to these cases, defendant contends (Def.'s Mem., pp. 30-35) that the foreign intelligence exception is "narrow" and applies only when the search is minimally intrusive and executive discretion is strictly confined. There is no such limitation on the doctrine. *Cf. MacWade v. Kelly*, 460 F.3d 260, 269 (2d Cir. 2006) (noting, in upholding under special needs doctrine warrantless subway searches to prevent terrorist attacks, that "[t]he Supreme Court never has implied – much less actually held – that a reduced privacy expectation is a *sine qua non* of special needs analysis"). While considerations of intrusiveness and executive discretion may be relevant to the reasonableness of a government program designed to serve a special need, neither factor is decisive regarding whether the doctrine applies at the threshold as an exception to the warrant clause. *See id.* at 268-69 (addressing such factors under the general reasonableness test, separately from the threshold question whether the searches served a governmental purpose distinct from ordinary law enforcement).

/ / /

---

acquisition in this case, which targeted non-United States person(s) reasonably believed to be outside the United States.

[23] The plurality in *Zweibon* specifically noted that the surveillance at issue targeted a domestic organization and suggested that its conclusion might be different if a foreign power were targeted. *See* 516 F.2d at 651.

Defendant relies extensively on the Supreme Court's decision in *United States v. United States District Court (Keith)*, 407 U.S. 297 (1972). This reliance is misplaced, as the Court in *Keith* expressly reserved the issue of a warrant requirement for foreign intelligence collection. As the FISA Court of Review recognized in *In re Sealed Case*, the Supreme Court explained in *Keith* that "the focus of security surveillance 'may be less precise than that directed against more conventional types of crime' even in the area of *domestic* threats to national security." 310 F.3d at 738 (emphasis in original); *see also 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"). The same rationale "applies *a fortiori* to foreign threats," a fact that Congress necessarily recognized in enacting FISA. *In re Sealed Case*, 310 F.3d at 738; *see also Truong*, 629 F.2d at 913 ("For several reasons, the needs of the executive are so compelling in the area of foreign intelligence, unlike the area of domestic security, that a uniform warrant requirement would, following *Keith*, 'unduly frustrate' the President in carrying out his foreign affairs responsibilities."). In addition, unlike the intelligence collection at issue here, the surveillance in *Keith* was conducted not only without a warrant but without any judicial or congressional oversight of any kind. *See Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 635-37 (1952) (Jackson, J. concurring) ("When the President acts pursuant to an express or implied authorization of Congress, his authority is at its maximum."). The courts that have addressed the issue of whether foreign intelligence collection is subject to a warrant requirement have expressly distinguished *Keith* in holding that it is not. *In re Directives*, 551 F.3d at 1010; *In re Sealed Case*, 310 F.3d at 744; *Truong*, 629 F.2d at 913; *Butenko*, 494 F.2d at 602 n.32; *Brown*, 484 F.2d at 425.

In sum, courts have generally recognized, by analogy to the "special needs" doctrine, that

a foreign intelligence exception to the warrant requirement exists. As the FISC has held, and for the reasons set forth below, that exception applies to acquisitions under Section 702. *[Caption Redacted]*, 2011 WL 10945618, at *24 (FISC Oct. 3, 2011) ("The Court has previously concluded that the acquisition of foreign intelligence information pursuant to Section 702 falls within the 'foreign intelligence exception' to the warrant requirement of the Fourth Amendment.").

c. The Government's Purpose in Section 702 Collection Goes Beyond Ordinary Crime Control

First, it is clear that the government's programmatic purpose in obtaining the information pursuant to Section 702 goes beyond routine law enforcement. *See In re Sealed Case*, 310 F.3d at 717 (holding that the government's "programmatic purpose" in obtaining foreign intelligence information is "to protect the nation against terrorist and espionage threats directed by foreign powers" – "a special need" that fundamentally differs from "ordinary crime control."); *see also Cassidy v. Chertoff*, 471 F.3d 67, 82 (2d Cir. 2006) (upholding warrantless searches of ferry passengers because "[p]reventing or deterring large-scale terrorist attacks present problems that are distinct from standard law enforcement needs and indeed go well beyond them"). Acquisitions under Section 702 must be conducted with a "significant purpose" to "obtain foreign intelligence information." As the FISA Court of Review found in the context of the PAA, the "stated purpose" of the collection "centers on garnering foreign intelligence," and "[t]here is no indication that the collections of information are primarily related to ordinary criminal-law enforcement purposes." The same is true of the collection authorized under Section 702 in this case.[24]

[24] **[CLASSIFIED MATERIAL REDACTED]**

d. A Warrant or Probable Cause Requirement Would Be Impracticable

Second, as the FISA Court of Review found with respect to the FAA's predecessor statute, "there is a high degree of probability that requiring a warrant would hinder the government's ability to collect time-sensitive information and, thus, would impede the vital national security interests that are at stake." *In re Directives*, 551 F.3d at 1011; *see also Truong*, 629 F.2d at 913 (noting that "attempts to counter foreign threats to the national security require the utmost stealth, speed, and secrecy" and, therefore, "[a] warrant requirement 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, and increase the chance of leaks regarding sensitive executive operations").[25] Changes in technology and the manner of collecting foreign intelligence information, as well as the shifting threat and communications methods employed by transnational terrorist groups, make it impracticable for the government to obtain traditional warrants or FISC orders for the acquisitions currently authorized under Section 702. Indeed, Congress enacted the FAA in part because the burden of preparing individualized FISA applications for intelligence collection targeting non-U.S. persons outside the United States was harming the government's ability to collect foreign intelligence information from targets overseas. *See* 124 Cong. Rec. S6097, S6122 (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.").

When the government has reason to believe that a non-U.S. person overseas is connected to international terrorist activities but the government lacks sufficient evidence to establish probable cause that the target is an agent of a foreign power, a warrant requirement could prevent

[25] **[CLASSIFIED MATERIAL REDACTED]**

the government from obtaining significant information. Even in circumstances where the government succeeded in eventually gathering enough information to establish probable cause under FISA, the need to develop such information and obtain approval of the FISC could result in delays that would hinder the government's ability to monitor fast-moving threats. *See In re Directives*, 551 F.3d at 1011-12 (Because of the government's "need for speed, stealth, and secrecy" in this context, "[c]ompulsory compliance with the warrant requirement would introduce an element of delay, thus frustrating the government's ability to collect information in a timely manner"); *cf. Verdugo-Urquidez*, 494 U.S. at 273-74 ("Application of the Fourth Amendment" to aliens abroad could "significantly disrupt the ability of the political branches to respond to foreign situations involving our national interest."); *Skinner v. Railway Labor Executives' Ass'n*, 489 U.S. 602, 623 (1989) (upholding warrantless search in part because "the delay necessary to procure a warrant . . . may result in the destruction of valuable evidence"). Finally, a warrant requirement in this context would impose significant burdens on the government, because substantial resources and time of national security personnel would be diverted to preparing individualized warrant applications targeting persons who lack Fourth Amendment rights. *Von Raab*, 489 U.S. at 666-67 (the mission of the Customs Service "would be compromised if it were required to seek search warrants in connection with routine, yet sensitive, employment decisions"); *O'Connor v. Ortega*, 480 U.S. 709, 722 (1987) (plurality opinion) ("requiring an employer to obtain a warrant" to access employee's office or files "would seriously disrupt the routine conduct of business and would be unduly burdensome").

In short, a warrant requirement would significantly undermine the government's ability to obtain foreign intelligence information vital to the Nation's security. *See Bin Laden*, 126 F. Supp. 2d at 273 ("[T]he imposition of a warrant requirement [would] be a disproportionate and

perhaps even disabling burden" on the government's ability to obtain foreign intelligence information). That would be a particularly unnecessary result because Section 702 collection may not intentionally target persons protected by the Fourth Amendment and the law contains robust safeguards that protect the interests of U.S. persons whose communications might be incidentally collected. *See United States v. Abu-Jihaad*, 630 F.3d 102, 121-22 (2d Cir. 2010) ("[T]he Constitution's warrant requirement is flexible, so that different standards may be compatible with the Fourth Amendment in light of the different purposes and practical considerations at issue.") (internal quotation marks and citation omitted).[26]

e. A Warrant Requirement Would Inappropriately Interfere with Executive Branch Discretion in the Collection of Foreign Intelligence

The Fourth Amendment's warrant requirement is based in part on the interest in "interpos[ing] a judicial officer between the zealous police officer ferreting out crime and the subject of the search." *In re Terrorist Bombings*, 552 F.3d at 170 n.7. But that concern is considerably diminished in this context because of "the acknowledged wide discretion afforded the executive branch in foreign affairs." *Id.*; *see Truong*, 629 F.2d at 914 ("[T]he executive branch not only has superior expertise in the area of foreign intelligence, it is also constitutionally designated as the pre-eminent authority in foreign affairs."). For that reason, the Fourth Amendment does not require that courts interpose themselves in the Executive Branch's collection of foreign intelligence beyond the procedures provided for by Congress.[27]

---

[26] Courts have recognized the continuing validity of the rationale for the foreign intelligence exception even after the enactment of FISA created a regime in which the government could obtain a court order to conduct foreign intelligence surveillance in certain circumstances. *See, e.g.*, *In re Directives*, 551 F.3d at 1010-11; *In re Sealed Case*, 310 F.3d at 742; *Duka*, 671 F.3d at 341; *[Caption Redacted]*, 2011 WL 10945618, at *24.

[27] Defendant contends (Def.'s Mem., p. 33) that application of the foreign intelligence exception here would "undermine the FISA's purpose of curbing 'the practice by which the Executive

3. The Government's Collection of Foreign Intelligence Information Pursuant to Section 702 Is Constitutional Under the Fourth Amendment's General Reasonableness Test

As explained above, incidental collection of communications of U.S. persons during an otherwise lawful collection does not render the collection constitutionally unreasonable. *See* Part IV.A.1.b. That principle applies here because the collection lawfully targeted non-U.S. persons outside the United States for foreign intelligence purposes. Moreover, as set forth below, even assuming that such incidental collection must satisfy the Fourth Amendment's "general reasonableness" test, the acquisitions at issue here were lawful under that test.

In circumstances where a warrant and probable cause are not required, searches and seizures are generally subject to the Fourth Amendment's "traditional standards of reasonableness." *Maryland v. King*, 133 S. Ct. at 1970; *see id.* ("To say that no warrant is required is merely to acknowledge that rather than employing a *per se* rule of unreasonableness, we balance the privacy-related and law enforcement-related concerns to determine if the intrusion was reasonable.") (internal quotation marks and citation omitted). In assessing the constitutional reasonableness of a government search, the court must weigh "the promotion of legitimate governmental interests against the degree to which [the search] intrudes upon an individual's privacy." *Id.* (internal quotation marks and citation omitted); *Knights*, 534 U.S. at 117-19 (describing balancing as "general Fourth Amendment approach"); *T.L.O.*, 469 U.S. at 337 (stating that "[t]he determination of the standard of reasonableness" requires balancing).

Branch may conduct warrantless electronic surveillance on its own unilateral determination that national security justifies it." (quoting S. Rep. No. 95-604(1) at 8). But Section 702 does not authorize "unilateral" Executive Branch surveillance, as the Supreme Court has recognized. *See Clapper*, 133 S. Ct. at 1144 ("Surveillance under § 1881a is subject to statutory conditions, judicial authorization, congressional supervision, and compliance with the Fourth Amendment."). In any event, even if defendant were correct that Section 1881a is inconsistent with statements in the legislative history of a previous version of FISA, the plain terms of the subsequent statute would prevail.

The court determines what is reasonable, and what safeguards may be necessary in a particular context, by balancing the interests at stake in light of "the totality of the circumstances." *Samson*, 547 U.S. at 848; *see also Von Raab*, 489 U.S. at 665, 668 (recognizing that "neither a warrant nor probable cause, nor, indeed, any measure of individualized suspicion, is an indispensable component of reasonableness in every circumstance" and that "the traditional probable-cause standard may be unhelpful" when the government "seeks to *prevent*" dangers to public safety); *In re Directives*, 551 F.3d at 1012 (reviewing collection under the PAA under the general reasonableness test).

Under the general reasonableness balancing test, searches without a warrant or individualized finding of probable cause are particularly likely to be found reasonable when the governmental need is especially great or especially likely to be frustrated by a warrant requirement, where the search involves modest intrusions on the individual's privacy, and where alternative safeguards restrain the government within reasonable limits. *See, e.g.*, *Illinois v. McArthur*, 531 U.S. 326, 330-31 (2001) ("When faced with special law enforcement needs, diminished expectations of privacy, minimal intrusions, or the like, the Court has found that certain general, or individual, circumstances may render a warrantless search or seizure reasonable."); *King*, 133 S. Ct. at 1969 (warrantless search may be reasonable where "the public interest is such that neither a warrant nor probable cause is required" or where "an individual is already on notice . . . that some reasonable [government] intrusion on his privacy is to be expected") (citation omitted); *Skinner*, 489 U.S. at 623-33.

The Supreme Court recently engaged in this kind of balancing in *King*, which involved warrantless searches of arrestees to obtain DNA samples. 133 S. Ct. at 1968-69. The Court examined the totality of the circumstances, weighed the various interests at stake, and concluded,

in light of the government's "substantial interest" in the "identification of arrestees," the diminished expectations of privacy of an individual taken into police custody, and statutory protections that limited the purposes for which the DNA evidence could be collected and stored, that the balance favored the government. *Id.* at 1977-80; *see also Samson*, 547 U.S. at 848-57 (applying reasonableness balance in upholding warrantless, suspicionless search of the person of a parolee).

In *In re Directives*, the FISA Court of Review applied the general reasonableness test in considering the constitutional reasonableness of the PAA, the FAA's predecessor statute, in the context of an as-applied challenge brought by a private party that had been directed by the government to assist in effectuating surveillance under the statute. 551 F.3d at 1012-15.[28] In balancing the respective interests, the FISA Court of Review recognized that the government's interest in national security was of such a "high[] order of magnitude" that it would justify significant intrusions on individual privacy. *Id.* at 1012. The FISA Court of Review noted further that the PAA, the certifications, and the directives contained a "matrix of safeguards," *id.* at 1013, including "effective minimization procedures" that were "almost identical to those used under FISA to ensure the curtailment of both mistaken and incidental acquisitions," *id.* at 1015, as well as "targeting procedures" that included "provisions designed to prevent errors" and

[28] The PAA was not identical to, and in certain respects was broader than, Section 702. Notably, the PAA authorized surveillance concerning "persons reasonably believed to be outside the United States" without distinguishing between U.S.- and non-U.S. persons, *In re Directives*, 551 F.3d at 1007, while Section 702 authorizes only surveillance targeting non-U.S. persons outside the United States. In addition, the petitioner in *In re Directives* limited its claims to alleged injuries to U.S. persons. Accordingly, the analysis in *In re Directives* addresses certain issues specific to foreign intelligence surveillance targeted at U.S. persons abroad, including a requirement that surveillance targeting U.S. persons be based on a finding by the Attorney General of probable cause to believe that the U.S. person was a foreign power or agent of a foreign power, that are not applicable here.

provided for Executive Branch and congressional oversight of "compliance with the targeting procedures," *id.* The FISA Court of Review concluded, based on the panoply of safeguards in the statutory provisions and implementing procedures, that "the surveillances at issue satisfy the Fourth Amendment's reasonableness requirement." *Id.* at 1016.[29]

The FAA provisions, certifications, and procedures at issue in this case, with respect to collection targeting non-U.S. persons overseas, are as protective as, and in some respects significantly more robust than, the comparable PAA procedures that the FISA Court of Review considered in holding that the directives issued under the PAA were constitutional.[30] In addition, the FAA goes beyond the PAA by requiring a prior finding by the FISC that the targeting and minimization procedures are reasonable under the Fourth Amendment. 50 U.S.C. § 1881a(i). The FAA, unlike the PAA, also expressly prohibits "reverse targeting" of U.S. persons. 50 U.S.C. § 1881a(b)(2). The FAA thus stands on an even firmer constitutional foundation than the PAA, and the FISA Court of Review's analysis upholding the latter applies also to the former. Defendant's motion does not distinguish, or even cite, the FISA Court of Review's opinion in *In re Directives*.

In addition, the FISC has repeatedly reviewed the targeting and minimization procedures governing the government's acquisition of foreign intelligence information under Section 702 and held that acquisitions pursuant to those procedures satisfy the Fourth Amendment reasonableness standard. *See [Caption Redacted]*, 2011 WL 10945618, at *6 (FISC Oct. 3, 2011) ("The Court found in those prior dockets that the targeting and minimization procedures

---

[29] *In re Directives* was not litigated *ex parte*. The FISA Court of Review considered briefing and oral argument from both the government and the communications provider that challenged the directives. *In re Directives,* 551 F.3d at 1008.

[30] **[CLASSIFIED MATERIAL REDACTED]**

were consistent with the requirements of [Section 702] and with the Fourth Amendment."). There is no reason for a different outcome here.

a. Acquisitions Under Section 702 Advance the Government's Compelling Interest in Obtaining Foreign Intelligence Information to Protect National Security

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; *see also [Caption Redacted]*, 2011 WL 10945618, at *25 (FISC Oct. 3, 2011); *Haig v. Agee*, 453 U.S. 280, 307 (1981) ("It is 'obvious and unarguable' that no governmental interest is more compelling than the security of the Nation.") (citation omitted). The terrorist threat the United States is facing today "may well involve the most serious threat our country faces." *In re Sealed Case*, 310 F.3d at 746; *see also Holder v. Humanitarian Law Project*, 130 S. Ct. 2705, 2724 (2010) ("[T]he Government's interest in combating terrorism is an urgent objective of the highest order."); *Duka*, 671 F.3d at 340 ("The government's interests in security and intelligence are entitled to particular deference."). Courts have recognized that the government's compelling interest in collecting foreign intelligence information to protect the Nation against terrorist groups and other foreign threats may outweigh individual privacy interests. *See, e.g., In re Terrorist Bombings*, 552 F.3d at 172-76 (upholding search and surveillance targeting U.S. person abroad because the intrusion on the individual's privacy was outweighed by the government's need to monitor the activities of al Qaeda); *Cassidy*, 471 F.3d at 82 (upholding warrantless searches of ferry passengers in light of government interest in "[p]reventing or deterring large-scale terrorist attacks").

The collection authorized by Section 702 is crucial to the government's efforts against terrorism and other threats both to the United States and its interests abroad. *See* National

Security Agency, *The National Security Agency: Missions Authorities, Oversight and Partnerships* 4 (August 9, 2013) ("[C]ollection under FAA Section 702 is the most significant tool in the NSA collection arsenal for the detection, identification, and disruption of terrorist threats to the U.S. and around the world."). As the Senate Select Committee on Intelligence found in recommending re-authorization of the FAA in 2012, "the authorities provided under the FISA Amendments Act have greatly increased the government's ability to collect information and act quickly against important foreign intelligence targets." S. Rep. No.174, 112th Cong., 2nd Sess. 2 (June 7, 2012); *see also id.* at 17 (noting that Section 702, in addition to "provid[ing] information about the plans and identities of terrorists" also enables the government to collect "information about the intentions and capabilities of weapons proliferators and other foreign adversaries who threaten the United States"). The Committee noted further that "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." *Id.*; *see also* H.R. Rep. 112-645 (II) 112th Cong., 2nd Sess. 3 (August 2, 2012) ("The importance of the collection of foreign intelligence under the FISA Amendments Act . . . cannot be underscored enough. . . . 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.").

A panel of experts appointed by the President to review the government's intelligence collection activities examined "the details of 54 counterterrorism investigations since 2007 that resulted in the prevention of terrorist attacks" and found that "[i]n all but one of these cases, information obtained under section 702 contributed in some degree to the success of the

investigation." The President's Review Group on Intelligence and Communications Technologies, *Liberty and Security in a Changing World* 144-45 (Dec. 12, 2013). The panel concluded that "[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." *Id.* at 145. Thus, as the Executive Branch, Congress, the FISC, and the President's Review Group have all recognized, the government has an extraordinarily compelling interest in conducting the collection authorized by Section 702.[31]

b. U.S. Persons Have Limited Expectations of Privacy in Electronic Communications with Non-U.S. Persons Outside the United States

Because surveillance under Section 702 must target non-U.S. persons reasonably believed to be located outside the United States (who generally lack Fourth Amendment rights), the only constitutional interests at stake are those of persons protected by the Fourth Amendment who were either mistakenly targeted under Section 702, or whose communications were incidentally collected in the course of the government's targeting of another person reasonably believed to be a non-U.S. person outside the United States. In the context of incidental collection, the privacy interests of U.S. persons in communications are significantly diminished when those communications have been transmitted to or obtained from non-U.S. persons located abroad.

The Supreme Court has long held that when one person voluntarily discloses information to another, the first person loses any cognizable interest under the Fourth Amendment in what the second person does with the information. *See United States v. Miller*, 425 U.S. 435, 443 (1976); *Couch v. United States*, 409 U.S. 322, 335 (1973); *White*, 401 U.S. at 752 (plurality opinion); *Hoffa v. United States*, 385 U.S. 293, 302-03 (1966). For Fourth Amendment

[31] **[CLASSIFIED MATERIAL REDACTED]**

purposes, the same principle applies whether the recipient intentionally makes the information public or stores it in a place subject to a government search. Thus, once a non-U.S. person located outside the United States receives information, the sender loses any cognizable Fourth Amendment rights with respect to that information. That is true even if the sender is a U.S. person protected by the Fourth Amendment, because he assumes the risk that the foreign recipient will give the information to others, leave the information freely accessible to others, or that the U.S. government (or a foreign government) will obtain the information.[32]

This rule applies to physical mail, even within the United States. Although, as defendant notes (Def.'s Mem. 17), the Fourth Amendment protects sealed letters in transit, "once a letter is sent to someone, 'the sender's expectation of privacy ordinarily terminates upon delivery.'" *United States v. Gordon*, 168 F.3d 1222, 1228 (10th Cir. 1999) (quoting *United States v. King*, 55 F.3d 1193, 1196 (6th Cir. 1995)). The same rule applies to email users, who lack "a legitimate expectation of privacy in an email that had already reached its recipient." *Guest v. Leis*, 255 F.3d 325, 333 (6th Cir. 2001); *see also United States v. Heckencamp*, 482 F.3d 1142, 1146 (9th Cir. 2007) (An "expectation of privacy may be diminished" for "transmissions over the Internet or email that have already arrived at the recipient.") (citation omitted); *United States v. Lifshitz*, 369 F.3d 173, 190 (2d Cir. 2004) (noting that a sender of email, like a letter-writer, would lose an objective expectation of privacy in email that the recipient had received).[33]

---

[32] The "recipient" in this context refers to the ultimate recipient, not (for example) an internet service provider. *See United States v. Warshak*, 631 F.3d 266, 282-88 (6th Cir. 2010). Thus, while *Warshak* held that a subscriber has a reasonable expectation of privacy in emails that the provider stores in the *subscriber's* account, it did not say that a person's Fourth Amendment rights are implicated when the government obtains, from the service provider, emails from *someone else*'s account.

[33] Moreover, any expectation of privacy of defendant in his electronic communications with a non-U.S. person overseas is also diminished by the prospect that his foreign correspondent could

[CLASSIFIED MATERIAL REDACTED]

Finally, the principles underlying the "border search" doctrine are also relevant to this Court's weighing of the individual's privacy interests relative to the government's interests in this context. Courts have long recognized the government's paramount interest in examining persons and property entering or exiting the country. *Flores-Montano*, 541 U.S. at 152. In that context, "not only is the expectation of privacy less," but also "the Fourth Amendment balance between the interests of the Government and the privacy right of the individual is also struck much more favorably to the Government." *United States v. Montoya de Hernandez*, 473 U.S. 531, 539-40 (1985) (citation omitted). Accordingly, under the rubric of the "border search" doctrine, courts have long recognized a diminished expectation of privacy in letters or packages that transit an international border, even where the search takes place in the interior of the country. *See United States v. Ramsey*, 431 U.S. 606, 620 (1977) (holding that the border search exception applies to international letters, because "[t]he critical fact is that the envelopes cross the border . . . not that they are brought in by one mode of transportation rather than another"); *United States v. Seljan*, 547 F.3d 993, 1003 (9th Cir. 2008) ("An envelope containing personal correspondence is not uniquely protected from search at the border."); *United States v. King*, 517

---

be a target for surveillance by foreign governments or private entities, whose activities are not governed by the United States Constitution or federal law, or by the U.S. Government, pursuant to various authorities applicable to foreign intelligence surveillance conducted abroad. *Cf. Clapper*, 133 S. Ct. at 1149 (noting that the government conducts surveillance of persons abroad under "programs that are governed by Executive Order 12333" and that "[t]he Government may also obtain information from the intelligence services of foreign nations"); *Amnesty Int'l USA v. Clapper*, 667 F.3d 163, 192 (2d Cir. 2011) (Raggi, J., dissenting) (Because "the United States is hardly the only government conducting electronic surveillance," the foreign contacts of plaintiffs challenging the FAA might "be prime targets for surveillance by other countries," especially foreign contacts "believed to be associated with terrorist organizations."); *Verdugo-Urquidez*, 494 U.S. at 278 (Kennedy, J., concurring) (noting the relevance of "differing and perhaps unascertainable conceptions of reasonableness and privacy that prevail abroad") This reality, which courts have acknowledged, arguably put defendant "on notice . . . that some reasonable [government] intrusion on his privacy is to be expected." *King*, 133 S. Ct. at 1969.

F.2d 350, 354 (5th Cir. 1975) ("Appellants here could have had no reasonable expectation that their letters, mailed from abroad, would remain uninspected.").

The same rationale applies also to international data transmissions, like the communications at issue here, because such transmissions, in the form of terrorist communications, cyber attacks, illegal financial transactions, and the like, may implicate national security or other government interests to a similar degree as physical mail in an envelope. *See Seljan*, 547 F.3d at 1001-03 (upholding suspicionless search of envelope containing personal correspondence in light of "tempered" expectation of privacy in international mail and the government's interest in "regulating the flow of persons and property across the border."). Although the government does not contend that the Section 702 collection here was per se reasonable under the border search doctrine, the point remains that the principles underlying that doctrine support the constitutional reasonableness of the collection at issue in this case.

c. The Privacy Interests of U.S. Persons Are Protected by Stringent Safeguards and Procedures

The government employs multiple safeguards that are designed to ensure that surveillance is appropriately targeted at non-U.S. persons located outside the United States for foreign intelligence purposes and to protect the privacy interests of U.S. persons who communicate with targets or whose communications are otherwise incidentally collected. These safeguards and procedures – some of which go beyond what courts have held reasonable in the context of "special needs" warrantless searches involving less compelling governmental interests – provide constitutionally sufficient protection for the privacy interests of U.S. persons.

i. Senior officials certify that the government's procedures satisfy statutory requirements

Section 702 requires the DNI and the Attorney General to certify that procedures are in

place to protect the privacy of U.S. persons, including targeting procedures and minimization procedures. 50 U.S.C. § 1881a(a), (g), and (i). In addition, the DNI and Attorney General must also certify, *inter alia*, that a significant purpose of the acquisition is to obtain foreign intelligence information, that the Attorney General and DNI have adopted guidelines to ensure compliance with the statutory limitations in Section 702(b), and that the targeting procedures, minimization procedures, and guidelines adopted by the government are consistent with the Fourth Amendment. 50 U.S.C. § 1881a(g)(2)(A). The requirement that these senior executive branch officials certify that the procedures comply with statutory requirements and with the Constitution represents an important "internal check" on the actions of the Executive Branch. *See In re Sealed Case*, 310 F.3d at 739.

ii. Targeting procedures ensure that the government targets only non-U.S. persons reasonably believed to be outside the United States

Section 702 provides that the targeting procedures must be "reasonably designed" to "ensure that any acquisition authorized under [the certification] is limited to targeting persons reasonably believed to be located outside the United States" and to "prevent 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 located in the United States." *See* 50 U.S.C. § 1881a(d)(1). The FISC repeatedly has found that the targeting procedures employed by the government meet that standard. *See supra* Part V.B.; *[Caption Redacted]*, 2011 WL 10945618, at *6 (FISC Oct. 3, 2011) ("The Court found in those prior dockets that the targeting and minimization procedures were consistent with the requirements of 50 U.S.C. § 1881(d)-(e) and with the Fourth Amendment.").

[CLASSIFIED MATERIAL REDACTED]

These detailed procedures refute defendant's contention that collection under Section 702 is unreasonably broad because the government "may target entire geographical areas or groups of people," or that the government could "intercept and read every American communication with a country of interest." (Def.'s Mem., p. 20-21). Those contentions amount to an accusation that the government will not abide by the required procedures, despite extensive oversight, and that the government will engage in "reverse targeting" of U.S. persons, even though that is expressly prohibited by the statute, *see* 50 U.S.C. § 1881a(b)(2). However, as the FISA Court of Review recognized, there is a "presumption of regularity" that "supports the official acts of public officers," and unless there is "clear evidence to the contrary, courts presume that they have properly discharged their official duties." *In re Directives*, 551 F.3d at 1011. In this case, as set forth more fully *infra* at Part V.D., there is no indication of any non-compliance by the government that would rebut that presumption.[34]

[CLASSIFIED MATERIAL REDACTED]

iii. Minimization procedures protect the privacy of U.S. persons whose communications are acquired

Section 702 requires the government to employ minimization procedures, as defined in FISA, to limit the acquisition, retention, and dissemination of information concerning U.S. persons. *See* 50 U.S.C. § 1801(h)(1). Section 702 further requires that the FISC review those procedures and determine that acquisitions in accordance with such procedures are consistent with the FAA and the Fourth Amendment. 50 U.S.C. § 1881a(i)(1) and (2).

The minimization procedures governing Section 702 collection, some of which have recently been declassified, are appropriately designed to minimize the acquisition, retention, and

[34] **[CLASSIFIED MATERIAL REDACTED]**

dissemination of information to, from, or about U.S. persons, consistent with the government's foreign intelligence needs. *See Minimization Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as amended* (dated October 31, 2011), dated October 31, 2011), available at www.dni.gov/files/documents/Minimization%20Procedures%20used%20by%20NSA%20in%20Connection%20with%20FISA%20SECT%20702.pdf ("NSA 2011 Minimization Procedures").[35] The procedures further require, among other things, that the identity of U.S. persons be redacted from intelligence reports prior to dissemination unless the information constitutes foreign intelligence information, is necessary to understand foreign intelligence information, or is evidence of a crime. *Id.* § 6(b). In other words, the procedures by design aim to ensure that any intrusion on the privacy of U.S. persons is reasonably balanced against the government's intelligence needs.

For the same reasons that courts have found the use of minimization procedures to be an important factor in holding traditional FISA surveillance to be reasonable under the Fourth Amendment, *In re Sealed Case*, 310 F.3d at 740-42, the use of substantially similar minimization procedures supports the reasonableness of surveillance under Section 702. *In re Directives*, 551 F.3d at 1015 (finding it "significant," in upholding the PAA, that "effective minimization procedures are in place" to "serve as an additional backstop against identification errors as well as a means of reducing the impact of incidental intrusions into the privacy of non-targeted United States persons.").[36]

/ / /

---

[35] **[CLASSIFIED MATERIAL REDACTED]**

[36] **[CLASSIFIED MATERIAL REDACTED]**

Defendant contends (Def.'s Mem., pp. 36-37) that the minimization procedures "ha[ve] no substantive content" and "provide no meaningful protection." However, the procedures employed here provide materially equivalent protection to the procedures employed for FISA Title I and III collection, and courts have found that these procedures sufficiently protect the privacy interests of U.S. persons whose communications are incidentally acquired. *In re Sealed Case*, 310 F.3d at 740-41; *see In re Directives*, 551 F.3d at 1015 (recognizing as "significant" to the Court's finding that acquisitions under the PAA were reasonable, that "effective minimization procedures are in place" that were "almost identical" to those used in traditional FISA surveillance). In addition, those procedures have repeatedly been found sufficient in the context of traditional FISA electronic surveillance and physical search, which target U.S. persons in the United States and therefore are more likely to capture communications of non-targeted U.S. persons than the foreign communications targeted under Section 702. *See [Caption Redacted]*, 2011 WL 10945618, at *7 (FISC Oct. 3, 2011).

The FISC has authority to supervise the government's compliance with minimization procedures. The FAA's oversight provisions require regular reporting to the FISC concerning the government's implementation of minimization procedures. 50 U.S.C. § 1881a(*l*). In addition, Rule 13(b) of the FISC's Rules of Procedures requires the government to report, in writing, all instances of non-compliance.[37] In response to such reports, the FISC has authority to disapprove or to require amendments to the minimization procedures, as, indeed, the FISC has done.[38]

---

[37] FISA Ct. R. of P. 13(b).

[38] In *[Caption Redacted]*, 2011 WL 10945618, at *1 (FISC Oct. 3, 2011), the FISC found that the government's minimization procedures, as applied to certain electronic communications acquired at "upstream" points on the internet backbone networks, did not comply with Section

Defendant further contends (Def.'s Mem., pp. 28-29) that, even assuming the government has lawfully acquired information pursuant to Section 702, any subsequent querying of a database containing that information (including queries using identifiers associated with U.S.-persons) amounts to a distinct Fourth Amendment "search" that requires a separate warrant.[39] Defendant is incorrect.

Courts have held in various contexts that where the government's querying of information that has lawfully been obtained does not implicate any reasonable expectation of privacy beyond that implicated in the initial collection, those queries do not constitute separate "searches" under the Fourth Amendment. *See United States v. Diaz-Castaneda*, 494 F.3d 1146, 1151-53 (9th Cir. 2007) (running computer query of individual's lawfully obtained license plate and driver's license identification numbers in government databases, which revealed information about subject's car ownership, driver status, and criminal record, was not a search under the Fourth Amendment); *Boroian v. Mueller*, 616 F.3d 60, 67-68 (1st Cir. 2010) ("[T]he government's retention and matching of [an individual's] profile against other profiles in [a DNA database] does not violate an expectation of privacy that society is prepared to recognize as reasonable, and thus does not constitute a separate search under the Fourth Amendment"); *see also Johnson v. Quander*, 440 F.3d 489, 498-99 (D.C. Cir. 2006) (holding that "accessing the records stored in the [DNA] database is not a 'search' for Fourth Amendment purposes" based in part on cases holding that, where a photograph is "taken in conformance with the Fourth

---

702 or the Constitution, due to technical limits on the government's ability to isolate targeted communications that were transmitted as part of a multi-communication batch. The government revised its procedures, and the FISC held that the amended procedures were consistent with the statute and the Fourth Amendment. *[Caption Redacted]*, 2011 WL 10947772, at *1 (FISC Nov. 30, 2011).
[CLASSIFIED MATERIAL REDACTED]

[39] **[CLASSIFIED MATERIAL REDACTED]**

Amendment, the government's storage and use of it does not give rise to an independent Fourth Amendment claim."). Notably, the Sixth Circuit has applied this principle in the foreign intelligence context. *Jabara v. Webster*, 691 F.2d 272, 277-79 (6th Cir. 1982) (holding, where plaintiff did not challenge the lawfulness of warrantless NSA interception of his foreign communications but challenged only the subsequent dissemination of the communications to the FBI, that such dissemination "after the messages had lawfully come into the possession of the NSA" did not implicate any reasonable expectation of privacy).[40]

The same reasoning applies here. Where, as here, the government has lawfully collected foreign intelligence information pursuant to statutory requirements and FISC-approved procedures that meet Fourth Amendment standards, the government's subsequent querying of that information does not amount to a significant further intrusion on privacy that implicates the Fourth Amendment. *See King*, 133 S. Ct. at 1980 (holding, "in light of the scientific and statutory safeguards" governing Maryland's warrantless collection of DNA from persons arrested for serious offenses, that "once respondent's DNA was lawfully collected," the subsequent analysis of the DNA "did not amount to a significant invasion of privacy that would render the DNA identification impermissible under the Fourth Amendment"); *see also Haskell v. Harris*, 2014 WL 1063399 at *4 (9th Cir. Mar. 20, 2014) (Smith, J, concurring) (noting that, under *King*, the differences between California's DNA statute and the Maryland statute at issue

[40] Defendant's contention (Def.'s Mem., pp.29-30) that "each stage of the process" including "retention, query, dissemination, use, and so forth" amounts to a separate search under the Fourth Amendment not only is contrary to these cases but also is impracticable, because, as the Sixth Circuit explained in *Jabara*, such a rule would require "a succession of warrants as information, lawfully acquired, is passed from one agency to another." 691 F.2d at 279; *see also id.* at 277 ("Evidence legally obtained by one police agency may be made available to other such agencies without a warrant, even for a use different from that for which it was originally taken.") (citation omitted). Accordingly, "[A]n expectation that information lawfully in the possession of a government agency will not be disseminated, without a warrant, to another government agency is [not] an expectation of privacy that society is prepared to recognize as reasonable." *Id.* at 279.

in *King* regarding when police may analyze DNA samples they had already obtained were "not constitutionally relevant"). Accordingly, the government's querying (whether using U.S. person identifiers or otherwise) of information lawfully obtained pursuant to Section 702 does not amount to a separate search under the Fourth Amendment and does not require separate or additional judicial process.

Defendant's reliance on cases holding that searches beyond the scope of consent, a warrant, or an initial private search require a separate warrant (Def.'s Mem., p. 29) is misplaced. In this case, as set forth in detail *infra* at Part V.D., the government complied with all applicable requirements in Section 702 and the FISC-authorized targeting and minimization procedures. The government's actions thus were within the scope of the relevant legal authority. For that reason, the cases defendant cites regarding circumstances where the government took actions beyond the scope of the warrant (or warrant exception) at issue are inapplicable here.

Finally, the fact that minimization procedures may permit the government to query information lawfully collected pursuant to Section 702 using identifiers associated with U.S. persons does not render those procedures constitutionally unreasonable. First, as noted above, the querying of information that the government lawfully has obtained is not a significant additional intrusion on a person's privacy, beyond the level of intrusion that has already resulted from the government's collection and review of the information pursuant to court-approved targeting and minimization procedures. Consistent with those procedures, the government is of course permitted to review the information it lawfully collects under Section 702 – which includes information concerning U.S. persons – to assess whether the information should be retained or disseminated. Accordingly, U.S.-person information is, by necessity, already subject to review (and use) under the court-approved minimization procedures. It would be perverse to

authorize the unrestricted review of lawfully collected information but then to restrict the targeted review of the same information in response to tailored queries. Querying lawfully collected information using U.S.-person identifiers does not involve a significant additional intrusion on a person's privacy, beyond the level of intrusion already occasioned by the government as it reviews and uses information it lawfully collects under Section 702 pursuant to its need to analyze whether the information should be retained or disseminated.

On the other side of the balance, the government has a compelling interest in conducting such queries for appropriate purposes including, for example, discovering potential links between foreign terrorist groups and persons within the United States in order to detect and disrupt terrorist attacks. *See* Part IV.A.3.a.[41] Similarly, the government's interest in preventing crime is "paramount," and a criminal investigation is always a "compelling" state interest. *Branzburg v. Hayes,* 408 U.S. 665, 700 (1972); *see also In re Directives*, 551 F.3d at 1011 ("A surveillance with a foreign intelligence purpose often will have some ancillary criminal-law purpose" because, for example, the "apprehension of terrorism suspects . . . is inextricably intertwined with the national security concerns that are at the core of foreign intelligence collection."). Likewise, the FISC repeatedly has approved minimization procedures that permit queries using U.S. person identifiers. *See [Caption Redacted]*, 2011 WL 10945618, at *7 (FISC Oct. 3, 2011). In approving such queries in the context of Section 702 collection, the FISC noted that the minimization procedures applicable to certain other FISA-acquired information, which the FISC had previously approved, similarly permit queries using U.S.-person identifiers, even though that information was likely to include a higher concentration of U.S. person information

[41] Such queries also help the government counteract an operational security measure like hiding operational communications in large amounts of non-operational communications in the hope of delaying the government's detection of those communications.

than Section 702 collection. *Id.* The FISC concluded, "[i]t follows that the substantially-similar querying provision found [in] the amended NSA minimization procedures should not be problematic in a collection that is focused on non-United States persons located outside the United States and that, in the aggregate, is less likely to result in the acquisition of nonpublic information regarding non-consenting United States persons." *Id.*[42]

In other words, surveillance under Title I of FISA is more likely to result in incidental collection of information about U.S. persons as to whom there has been no finding of probable cause that the individual is either an agent of a foreign power or engaged in criminal activity. Yet the FISC has long approved the querying of Title I data, including with U.S.-person identifiers, when such queries are designed to yield foreign intelligence information or evidence of a crime. Likewise, for decades the Federal Wiretap Act's minimization procedures have specifically allowed the government to search for and use evidence from a wiretap to prove a crime unrelated to the original purpose for the wiretap. *See* 18 U.S.C. § 2517(5); *see also, e.g., United States v. Goffer*, 721 F.3d 113, 124 (2d Cir. 2013). In sum, the government's querying of information lawfully acquired under Section 702 pursuant to the court-approved minimization procedures is reasonable under the Fourth Amendment, as the FISC has repeatedly found.

iv. A significant purpose of the acquisition must be to obtain foreign intelligence information

Section 702 only authorizes collection when a "significant purpose" of the collection is to "obtain foreign intelligence information." 50 U.S.C. § 1881a(g)(2)(A)(v). That requirement precludes the government from using directives issued under Section 702 "as a device to investigate wholly unrelated ordinary crimes." *In re Sealed Case*, 310 F.3d at 736.

[CLASSIFIED MATERIAL REDACTED]

[42] **[CLASSIFIED MATERIAL REDACTED]**

v. Executive Branch, Congressional, and Judicial Oversight

Section 702 requires the Attorney General and DNI to periodically assess the government's compliance with both the targeting and minimization procedures and with relevant compliance guidelines, including, for example, the extent to which U.S. persons' communications have been acquired under the statute and the number of intelligence reports stemming from Section 702 acquisitions referring to the identity of a U.S. person. *See* 50 U.S.C. § 1881a(*l*). They must submit those assessments both to the FISC and to congressional oversight committees. *Id.* The Attorney General must also keep the relevant oversight committees "fully inform[ed]" concerning the implementation of Section 702. 50 U.S.C. § 1881f(a) and (b)(1); *see also Clapper*, 133 S. Ct. at 1144 ("Surveillance under § 1881a is subject to statutory conditions, judicial authorization, congressional supervision, and compliance with the Fourth Amendment.").

In 2012, the Senate Select Committee on Intelligence, following four years of such oversight, found that

> [T]he assessments, reports, and other information obtained by the Committee demonstrate that the government implements the FAA surveillance authorities in a responsible manner with relatively few incidents of non-compliance. Where such incidents have arisen, they have been the inadvertent result of human error or technical defect and have been promptly reported and remedied. Through four years of oversight, the Committee has not identified a single case in which a government official engaged in a willful effort to circumvent or violate the law. Moreover, having reviewed opinions by the FISA Court, the Committee has also seen the seriousness with which the Court takes its responsibility to carefully consider Executive Branch applications for the exercise of FAA surveillance authorities.

S. Rep. No.174, 112th Cong. 2d Sess. 7 (June 7, 2012); *see also* H.R. Rep. No. 645(II), 112th Cong., 2d Sess. 4 ("The oversight this committee has conducted since the FAA was enacted in 2008 has shown no evidence that the Intelligence Community has engaged in any intentional or

willful failure to comply with statutory requirements or Executive Branch policies and procedures."). Under the FAA, as in traditional FISA, the "in-depth oversight of FISA surveillance by all three branches of government" helps to "ensure[]" the "privacy rights of individuals" and to "reconcile national intelligence and counterintelligence needs with constitutional principles in a way that is consistent with both national security and individual rights." *United States v. Belfield*, 692 F.2d 141, 148 (D.C. Cir. 1982).

vi. Prior Judicial review

Finally, Section 702 requires the FISC to enter an order approving the certification and the use of the targeting and minimization procedures if the court finds that the certification contains all the required elements, and that the targeting and minimization procedures are consistent with the requirements of 50 U.S.C. §§ 1881a(d) and (e) and with the Fourth Amendment. 50 U.S.C. § 1881a(i)(3)(A). The requirement of prior FISC approval, and in particular the requirement of a judicial finding that the government's targeting and minimization procedures are consistent with the Fourth Amendment, support a finding that Section 702 collection conducted pursuant to such procedures is constitutional. *See Clapper*, 133 S. Ct. at 1150 (noting the importance of the requirement that the FISC "assess whether the Government's targeting and minimization procedures comport with the Fourth Amendment"); *see also Clapper*, 667 F.3d at 190 (Raggi, J., dissenting) ("There is no reason to think that the Article III judges who serve on the FISA court will be timid in exercising this review authority"). Indeed, the FISC's declassified opinions make clear that the FISC takes seriously its responsibility to independently review the constitutional reasonableness of the applicable procedures and subjects those procedures to exacting scrutiny. *See, e.g., [Caption Redacted],* 2011 WL 10945618 (FISC Oct. 3, 2011).

d. Collection Under Section 702 Has Sufficient Particularity

Defendant's overarching argument is, in essence, that collection pursuant to Section 702 fails the Fourth Amendment's general reasonableness test because it does not require a particularized court order or finding of probable cause as in traditional FISA collection or domestic law enforcement wiretaps under Title III. (Def.'s Mem., pp. 16-28). In doing so, defendant describes Section 702-authorized collection as "dragnet" surveillance that collects communications in "bulk." (*See, e.g.*, *id.* at 8). However, collection under Section 702 is *not* bulk collection. Rather, it is targeted and particularized because FISC-approved procedures require the government to determine (1) that the particular "user of the facility to be tasked for collection is a non-United States person reasonably believed to be located outside the United States," *[Caption Redacted]*, 2011 WL 10945618, at *7 (FISC Oct. 3, 2011); and (2) the collection is designed to obtain foreign intelligence information within the scope of the certification approved by the court.[43]

[43] Indeed, a review of the various "transparency reports" recently published by various U.S. Internet Service Providers demonstrates that collection of communications' content pursuant to FISA orders and FAA directives is far from bulk "dragnet" surveillance. For example, Microsoft reported receiving "fewer than 1,000 FISA orders" (which Microsoft defines to include both traditional FISA orders and FAA directives that were received or active during the reporting period) that related to between 16,000 and 16,999 user accounts during the six-month period between July and December 2012. *See* Brad Smith, General Counsel and Executive Vice President, Legal and Corporate Affairs, Microsoft, "Providing additional transparency on U.S. government requests for customer data" (Feb. 3, 2014), available at, http://blogs.technet.com/b/microsoft_on_the_issues/archive/2014/02/03/providing-additional-transparency-on-US-government-requests-for-customer-data.aspx. A particular user may have multiple accounts, so this "does not necessarily mean that more than [16,000] people were covered by these data requests." *Id.* Rather, "this number will likely overstate the number of individuals subject to government orders." *Id.* The number of user accounts impacted by the same number of orders during other six-month reporting periods was even less, namely up to 15,999 between January and June 2013 and up to 11,999 between July and December 2011 and January to June 2012. *Id.* When balanced against the "hundreds of millions" of Microsoft customers, "only a fraction of a percent of [Microsoft] users are affected by these orders. In

[CLASSIFIED MATERIAL REDACTED]

Moreover, defendant's argument conflates the test for constitutional reasonableness with the *different* requirements for a warrant under the Fourth Amendment. *See* U.S. Const. Amend IV ("[N]o warrants shall issue, but upon probable cause, supported by Oath or Affirmation, *and particularly describing the place to be searched*) (emphasis added). In *In re Directives*, the FISA Court of Review emphatically rejected the petitioner's "invitation to reincorporate into the foreign intelligence exception the same warrant requirements that we already have held inapplicable." 551 F.3d at 1013. Although particularity may be considered as one factor among many in assessing the reasonableness of a particular search, the Fourth Amendment "imposes no irreducible requirement" of individualized suspicion where the search is otherwise reasonable, as it is here. *See King*, 133 S. Ct. at 1969. Moreover, as the FISA Court of Review found in the context of the PAA, the "matrix of safeguards," including robust targeting and minimization procedures, provide constitutionally sufficient protections for the same interests that would be served by requirements of particularity or prior judicial review of individual targets. *In re Directives*, 551 F.3d at 1013.[44]

/ / /

---

short, this means that we have not received the type of bulk data requests that are commonly discussed publicly regarding telephone records." *Id.*

[44] Defendant also contends (Def.'s Mem., pp. 26-28) that Section 702 violates the Fourth Amendment's notice requirement because targets need not be notified of the surveillance or search unless and until fruits of the surveillance or search are to be used in criminal prosecutions. This argument is meritless because FISA's Title I and Title III provisions have the same notice standards as Section 702 and courts have held that those provisions are reasonable. *See Belfield*, 692 F.2d at 145 n.8 ("[N]otice that the surveillance has been conducted, even years after the event, may destroy a valuable intelligence advantage."); *In re Sealed Case*, 310 F.3d at 741-42, 746 (FISA's notice provisions are reasonable and do not violate the Fourth Amendment). In any event, defendant has now received notice and has not alleged any prejudice caused by his not receiving notice earlier. *See* Government's Response to Defendant's Motion for Vacation of Conviction and Alternative Remedies, pp. 14-15.

In sum, in enacting Section 702, Congress and the Executive Branch developed a framework of procedures to facilitate collection of foreign intelligence vital to the nation's security while protecting any constitutionally protected privacy interests implicated by the collection. That framework is entitled to the utmost constitutional respect by this Court. *See Sawyer*, 343 U.S. at 635-37 (Jackson, J., concurring); *In re Directives*, 551 F.3d at 1016 ("[W]here the government has instituted several layers of serviceable safeguards to protect individuals against unwarranted harms and to minimize incidental intrusions, its efforts to protect national security should not be frustrated by the courts."). The safeguards built into the statute and the certifications and procedures by which it was implemented here ensured that the collection targeted only foreign person(s) outside the United States and was conducted in a way that only incidentally implicated the privacy of U.S. persons. Evaluating the totality of the circumstances and weighing the compelling governmental interests at stake in combination with the extensive safeguards employed by the government to protect the privacy interests of U.S. persons – including (1) certifications by Executive Branch officials concerning the permissible foreign intelligence purposes of the collection; (2) targeting procedures designed to ensure that only non-U.S. persons abroad are targeted; (3) minimization procedures to protect the privacy of U.S. persons whose communications are incidentally acquired; (4) the requirement of a significant purpose to obtain foreign intelligence information; (5) extensive oversight within the Executive Branch, as well as by Congress and the FISC; and (6) a prior judicial finding that the targeting and minimization procedures are consistent with the Fourth Amendment – this Court should hold that the government's acquisition pursuant to Section 702 of the foreign intelligence information challenged by defendant meets the Fourth Amendment's central requirement of reasonableness.

B. SECTION 702 DOES NOT AUTHORIZE THE FISC TO ISSUE "ADVISORY OPINIONS," NOR DOES IT VIOLATE THE NONDELEGATION DOCTRINE

Defendant contends (Def.'s Mem., pp. 24-26) that the FISC does not perform a proper judicial role under Article III in reviewing targeting and minimization procedures pursuant to Section 702 because the court does not review the procedures in the context of a particular proposed target and interception. Defendant further maintains that review at this level of generality does not present a "case or controversy" within the meaning of Article III and also violates the non-delegation doctrine. Those contentions have no merit.

"Article III courts perform a variety of functions not necessarily or directly connected to adversarial proceedings in a trial or appellate court." *Mistretta v. United States*, 488 U.S. 361, 389 n.16 (1989); *see also Morrison v. Olson*, 487 U.S. 654, 679 n.16 (1988). In particular, the courts have long participated in the oversight of government searches and surveillance by reviewing warrant and wiretap applications, notwithstanding that these proceedings are wholly *ex parte* and do not occur at the behest of an aggrieved party as ordinarily required for a "case or controversy" under Article III. *Mistretta*, 488 U.S. at 389 n.16; *see also, e.g.*, *In re Sealed Case*, 310 F.3d at 732 n.19 ("In light of [*Morrison* and *Mistretta*], we do not think there is much left to an argument . . . that the statutory responsibilities of the FISA court are inconsistent with Article III case and controversy responsibilities of federal judges because of the secret, non-adversary process."); *Matter of Kevork*, 634 F. Supp. 1002, 1014 (C.D. Cal. 1985) ("The *ex parte* nature of FISC proceedings is . . . consistent with Article III."), *aff'd*, 788 F.2d 566 (9th Cir. 1986).[45]

[45] The judiciary participates in oversight of searches and seizures not only by reviewing applications and issuing warrants, but also through its participation in promulgating the procedural rules governing the warrant process. *See* Fed. R. Crim. P. 41; *Mistretta*, 488 U.S. at 387-88 (noting that Congress may properly delegate to the courts the authority to prescribe rules of procedure in criminal cases).

Congress, in assigning the FISC an analogous function in Section 702, did not vest the FISC with a power that is "incongruous" with the judicial function or that "more appropriately belong[s] to another Branch" – the central question in a separation of powers challenge under Article III. *Mistretta*, 488 U.S. at 390; *see also In re Application of the U.S. for an Order Pursuant to 18 U.S.C. § 2703(d)*, 830 F. Supp. 2d 114, 144 (E.D. Va. 2011) ("Grand Juries, search warrants, wiretap orders, and many other *ex parte* applications and orders rely on judicial review to protect the rights of potential subjects of investigation. All of these tools have been routinely and consistently approved by the courts."). Congress's decision to vest the FISC with jurisdiction to review the reasonableness of procedures for searches or surveillance under the FAA is perfectly consistent with the traditional function of Article III courts in protecting the privacy rights of persons whose interests are potentially implicated by proposed searches, seizures, or compulsory processes. *Cf. Mistretta*, 488 U.S. at 390-91 (given the judiciary's traditional role in determining individual criminal sentences, the judiciary could constitutionally participate in formulating general sentencing guidelines).

Moreover, the decision the FISC is called upon to render under Section 702 is not merely "advisory," any more than a decision on a traditional search warrant or wiretap application is "advisory." If the FISC disapproves the government's proposed targeting or minimization procedures under Section 702, that decision has legal effect, because it bars the government from conducting collections under the statute if it does not remedy the deficiency within thirty days. A FISC order approving the proposed certification and procedures also has an effect on third parties, because it authorizes the government to issue directives (compulsory process analogous to a subpoena) to electronic communications service providers. The fact that the providers have a right to challenge a directive in court further establishes that a FISC order approving a Section

702 certification is not an advisory opinion but a legally enforceable order potentially subject to legal challenge. *See Clapper*, 133 S. Ct. at 1154 ("[A]ny electronic communications service provider that the Government directs to assist in § 1881a surveillance may challenge the lawfulness of that directive before the FISC.").

Defendant is also incorrect in claiming that the FISC's *ex parte* review of the government's certification violates the nondelegation doctrine and generally renders the issue inappropriate for resolution by an Article III judge. The nondelegation doctrine is satisfied when the challenged statute sets forth an "intelligible principle" that "clearly delineates" the boundaries of th[e] delegated authority." *Mistretta*, 488 U.S. at 372-73.[46] That standard is met here.

Section 702 requires the FISC to review specific targeting and minimization procedures to determine whether they comply with applicable statutory standards and the Fourth Amendment. Those are "intelligible principles." Moreover, that review is not conducted in the abstract; rather, the FISC must review the minimization procedures "in light of the purpose and technique of the *particular* surveillance." 50 U.S.C. § 1801(h)(1) (emphasis added); *see also id.* § 1821(4)(A) (requiring that minimization procedures with respect to physical search must be "reasonably designed in light of the purpose and technique of the *particular* physical search") (emphasis added). Accordingly, the FISC's review must consider the particular "purpose," as set forth in the certification, of the acquisitions, as well as the particular "technique[s]" the government uses. This often involves a close consideration of the application of specific, detailed provisions in the targeting and minimization procedures as applied to specific, technical

[46] As the Supreme Court has repeatedly observed, it has found only two statutes that lacked the necessary "intelligible principle" – and it has not found any in the last 70 years. *Whitman v. Am. Trucking Ass'ns*, 531 U.S. 457, 474 (2001).

tools through which the government implements Section 702. *See [Caption Redacted]*, 2011 WL 10945618, at *9 (FISC Oct. 3, 2011) ("The Court has repeatedly noted that the government's targeting and minimization procedures must be considered in light of the communications actually acquired."). That level of particularity and detail is exemplified in the declassified FISC opinions addressing the adequacy of particular targeting and minimization procedures in the context of certain technical limitations in the NSA's "upstream collection" of Internet communications transmitted as part of a multi-communication batch.[47] *See id.* at *9-*10.

Analyzing the reasonableness of electronic surveillance, in light of the government's national security interests and the privacy interests of potential subjects of the surveillance, is a traditional judicial function. *See Halperin v. Kissinger*, 606 F.2d 1192, 1201 n.59 (D.C. Cir. 1979) ("[D]etermin[ing] whether electronic surveillance was consonant with statutory and constitutional strictures [is] a traditional judicial function that is governed by well established and manageable standards."). The closely related question of whether surveillance conducted pursuant to particular procedures is reasonable under the relevant statutory and constitutional standards is also the kind of analysis that courts regularly undertake, such as, for example, when they adjudicate the constitutionality of a state statute regulating domestic wiretaps. *See United States v. Tortorello*, 480 F.2d 764, 772-73 (2d Cir. 1973) (analyzing constitutional adequacy of procedures provided by New York electronic surveillance statute).

The FISC's role under Section 702 is also analogous to judicial review of administrative warrants in the public health context, which may be based on the court's determination of the reasonableness of the standards and procedures for conducting inspections in a given area, rather

[47] **[CLASSIFIED MATERIAL REDACTED]**

than evidence of a violation at a specific location. *See Camara v. Municipal Ct.*, 387 U.S. 523, 537-38 (1967) ("Such standards, which will vary with the municipal program being enforced, may be based upon the passage of time, the nature of the building (e.g., a multifamily apartment house), or the condition of the entire area, but they will not necessarily depend upon specific knowledge of the condition of the particular dwelling."). Although warrant or wiretap applications for law enforcement purposes typically involve a more fact-specific form of review, that is because the Fourth Amendment or Title III requires more particularity in those contexts – not because of anything in Article III.

C. SECTION 702 DOES NOT VIOLATE THE FIRST AMENDMENT

Defendant contends (Def.'s Mem., pp. 37-39) that Section 702 violates the First Amendment because it has "deeply chilled" Americans' exercise of First Amendment rights through communications on the internet. That claim should be rejected.

First, defendant does not claim that Section 702 has had any effect on his own First Amendment rights. Instead, he claims (Def.'s Mem., p. 38) that the statute has an unconstitutional chilling effect on Americans generally and on various specific third parties, including his attorney and former President Jimmy Carter. Such claims do not provide a basis for exclusion of evidence. Although the Supreme Court has fashioned exclusionary rules for evidence obtained in violation of defendants' Fourth Amendment rights or Fifth Amendment *Miranda* rights, defendant cites no case in which a court has excluded evidence on the ground that it was obtained under a statute that unconstitutionally chills the First Amendment rights of third parties. *See United States v. Aguilar*, 883 F.2d 662, 697 (9th Cir. 1989) (noting that defendant's claim that evidence should be suppressed "is a *Fourth* Amendment claim, rather than a First") (citation omitted); *Abell v. Raines*, 640 F.2d 1085, 1088 (9th Cir. 1981) (rejecting

suppression claim based on alleged First Amendment violations in government investigation because "the Fourth Amendment (and the exclusionary rule) provide the only basis" upon which the evidence could have been excluded); *cf. United States v. Mayer*, 503 F.3d 740, 747 (9th Cir. 2007) ("We have not found any cases where an indictment was dismissed because the preceding investigation allegedly violated the *First Amendment* rights of a third party.").

Further, the Supreme Court and Ninth Circuit have held that when the government's investigative activities have an effect on individuals' First Amendment interests, those interests are safeguarded by adherence to Fourth Amendment standards. *Zurcher v. Stanford Daily*, 436 U.S. 547, 564 (1978) (requiring only that the Fourth Amendment be applied with "scrupulous exactitude" where First Amendment interests are implicated by a search); *Mayer*, 503 F.3d at 747-48 (noting that the "*Fourth Amendment* provides the relevant benchmark" for a challenge to a criminal investigation on First Amendment grounds); *see also Redd v. City of Enterprise*, 140 F.3d 1378, 1383-84 (11th Cir. 1998); *Reporters Comm. For Freedom of the Press v. AT&T*, 593 F.2d 1030, 1054-59 (D.C. Cir. 1978); *Jabara v. Kelley*, 476 F. Supp. 561, 572 (E.D. Mich. 1979) ("[T]he first amendment and the fourth amendment provide coextensive zones of privacy in the context of a good faith criminal investigation," including warrantless electronic surveillance by NSA and FBI), *vacated on other grounds*, 691 F.2d 272 (6th Cir. 1982).

Accordingly, "surveillance consistent with Fourth Amendment protections in connection with a good faith law enforcement investigation does not violate First Amendment rights, even though it may be directed at communicative or associative activities." *Gordon v. Warren Consol. Bd. of Educ.*, 706 F.2d 778, 781 n.3 (6th Cir. 1983) (collecting cases); *see Mayer*, 503 F.3d at 750 (explaining that undercover surveillance lawful under the Fourth Amendment does not violate First Amendment rights); *ACLU Found. of S. Cal. v. Barr*, 952 F.2d 457, 471 (D.C.

Cir. 1991) (same in context of FISA surveillance); *cf. Ramsey*, 431 U.S. at 623-24 (customs officers' inspection of international mail, without reading the correspondence, did not violate the First Amendment). As set forth above, the government's collection of foreign intelligence information under Section 702 does not violate the Fourth Amendment. And because defendant does not allege, and cannot show, that the government has conducted such collection with any purpose to suppress expressive or associative activity, the collection at issue does not violate the First Amendment.

Even if defendant could properly bring an independent First Amendment overbreadth claim in this context, he must show that the statute's "overbreadth [is] *substantial*, not only in an absolute sense, but also relative to [its] plainly legitimate sweep." *United States v. Williams*, 553 U.S. 285, 292 (2008); *see also id.* (noting that this requirement is "vigorously enforced"). Defendant has not made such a showing. To the contrary, defendant's overbreadth claim relies on the same allegation – that people will alter their behavior because they fear the possibility that their communications will be incidentally acquired under Section 702 – that the Supreme Court found to be too speculative to establish a cognizable injury. *See Clapper*, 133 S. Ct. at 1152 (plaintiffs could not bring constitutional challenge to Section 702 based on allegations that subjective fear of surveillance under Section 702 would deter plaintiffs from "conducting constitutionally protected activities") (citation omitted). Moreover, as the Supreme Court recognized, the self-censorship and countermeasures that defendant claims are caused by fear of Section 702 surveillance are "not fairly traceable" to that statute because "[t]he government has numerous other methods of conducting surveillance" of non-U.S. persons overseas in addition to Section 702. *Id.* at 1149, 1151.

Finally, although "constitutional violations may arise from the chilling effect of

regulations that fall short of a direct prohibition against the exercise of First Amendment rights," *id.* at 1152 (internal quotation marks omitted), the Court has not recognized constitutional violations based on chilling effects that allegedly "aris[e] merely from the individual's knowledge that a governmental agency was engaged in certain activities or from the individual's concomitant fear that, armed with the fruits of those activities, the agency might in the future take some *other* and additional action detrimental to that individual." *Id.* at 1152 (quoting *Laird v. Tatum*, 408 U.S. 1, 11 (1972)). Because Section 702 does not "regulate, constrain, or compel any action" by an individual, *id.* at 1153, the mere subjective fear of surveillance under that statute does not amount to a constitutionally significant burden on the exercise of First Amendment rights.

D. THE GOOD-FAITH EXCEPTION APPLIES

The good-faith exception to the exclusionary rule set forth in *United States v. Leon*, 468 U.S. 897, 913 (1984), provides an independent basis for denying defendant's suppression motion. *See, e.g., United States v. Ning Wen*, 477 F.3d 896, 897-98 (7th Cir. 2007) (applying good-faith exception to a claim that FISA surveillance violated the Fourth Amendment). The good-faith rule applies when law enforcement agents act in "objectively reasonable reliance on a statute" authorizing warrantless searches that is later deemed unconstitutional, *Illinois v. Krull*, 480 U.S. 340, 349-50 (1987), when law enforcement officers reasonably rely on the probable-cause determination of a neutral magistrate, *see Leon*, 468 U.S. at 920, and when law enforcement officers reasonably rely on then-binding appellate precedent that is subsequently overturned, *see Davis v. United States*, 131 S. Ct. 2419, 2434 (2011).

The good-faith exception applies here because the collection at issue was authorized by a duly enacted statute, an order issued by a neutral magistrate, and court of appeals precedent.

First, government agents conducted the collection at issue here pursuant to Section 702, as well as under procedures adopted by the Attorney General pursuant to the statute. *See Krull*, 480 U.S. at 349; *Duka*, 671 F.3d at 346 (reasoning that the good-faith rule applies because the search "was conducted in objectively reasonable reliance on a duly authorized statute [FISA]"); *see also United States v. Marzook*, 435 F. Supp. 2d 778, 790-91 (N.D. Ill. 2006) (holding that "the FBI's reliance on the Attorney General's approval under Executive Order 12,333 — an order that no court has found unconstitutional — was [ ] objectively reasonable because that order pertains to foreign intelligence gathering"). Second, the agents also reasonably relied on orders issued by neutral magistrates — the judges of the FISC — who repeatedly have held that the applicable targeting and minimization procedures are reasonable under the Fourth Amendment. *See Leon*, 468 U.S. at 920; *see also Duka*, 671 F.3d at 347 n.12 ("[O]bjective . . . reliance on the statute in this case is further bolstered by the fact that the particular provision at issue has been reviewed and declared constitutional by several courts."); *United States v. Mubayyid*, 521 F. Supp. 2d 125, 140 n.12 (D. Mass. 2007) (applying the good-faith exception because "there appears to be no issue as to whether the government proceeded in good faith and in reasonable reliance on the FISA orders"). Finally, the agents reasonably relied on appellate precedent from the FISA Court of Review that upheld similar directives issued under the PAA. *See Davis*, 131 S. Ct. at 2433-34; *In re Directives*, 551 F.3d at 1016.

Defendant cannot show that Section 702 is so "clearly unconstitutional," *Krull*, 480 U.S. at 349, that "a reasonable officer should have known that the statute was unconstitutional," *id.* at 355. Nor can he show that the collection was the result of "systemic error or reckless disregard of constitutional requirements." *Herring v. United States*, 555 U.S. 135, 147 (2009). Accordingly, even if the collection were deemed unconstitutional, the evidence derived from that

collection would not be subject to exclusion.[48]

V. THE FAA INFORMATION WAS LAWFULLY ACQUIRED AND CONDUCTED IN CONFORMITY WITH AN ORDER OF AUTHORIZATION OR APPROVAL

In addition to challenging the general constitutionality of Section 702, defendant also questions the government's compliance with the applicable targeting and minimization procedures with respect to the specific information used in his case. (Def.'s Mem., pp. 39-40). As explained below, this Court's *in camera, ex parte* review of the relevant classified materials will establish that the Section 702 acquisition was lawfully authorized and conducted. First, the applicable certifications, targeting procedures, and minimization procedures, all of which were reviewed and approved by the FISC, complied with the requirements for such certifications and procedures set forth in Section 702. Second, the Section 702 collection at issue in this case was conducted in accordance with those approved certifications and procedures.

A. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

/ / /

---

[48] In the related context of Title III of the Wiretap Act, the weight of the precedent establishes that Title III's statutory suppression remedy for criminal wiretap orders incorporates the good-faith exception. *See United States v. Moore*, 41 F.3d 370, 374, 376 (8th Cir. 1994) (applying good-faith exception to Title III violation); *United States v. Malekzadeh*, 855 F.2d 1492, 1497 (11th Cir. 1988) (same); *United States v. Brewer*, 204 Fed. Appx. 205 (4th Cir. 2006) (same); *United States v. Solomonyan*, 451 F. Supp. 2d 626, 637-38 (S.D.N.Y. 2006) (collecting cases). Although two courts of appeals have held otherwise, both courts also questioned in those cases whether the government's actions were actually taken in "good faith," either because the affiant recklessly misled the court, *see United States v. Rice*, 478 F.3d 704, 709-11 (6th Cir. 2007); or because the wiretap order, in the court's view, plainly violated the applicable rule, *see United States v. Glover*, 736 F.3d 509, 515-16 (D.C. Cir. 2013). In this case, even if some aspect of the collection did not comply with the requirements of Section 702, there is no similar indication of deliberate, reckless, or systemically negligent conduct. Accordingly, absent a finding that the government personnel who carried out the collection did not rely in good faith on the targeting and minimization procedures as approved by the FISC, or otherwise engaged in culpable conduct warranting application of the exclusionary rule, defendant's motion to suppress should be denied.

B. THE APPLICABLE TARGETING PROCEDURES MET THE STATUTORY REQUIREMENTS

Section 702 targeting procedures must be "reasonably designed" both to "ensure that any acquisition authorized [pursuant to Section 702] is limited to targeting persons reasonably believed to be located outside the United States" and to "prevent 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 located in the United States." 50 U.S.C. § 1881a(d)(1).

[CLASSIFIED MATERIAL REDACTED]

C. THE APPLICABLE MINIMIZATION PROCEDURES MET THE STATUTORY REQUIREMENTS

Section 702 requires the adoption of minimization procedures that comply with FISA's definition of such procedures. *See* 50 U.S.C. § 1881a(e)(1). That definition in turn requires that the minimization procedures must be reasonably designed, in light of the purpose and technique of the particular surveillance, in order to minimize any acquisition of non-publicly available information about unconsenting U.S. persons, and to minimize the retention and prohibit the dissemination of any such information that might still be acquired, consistent with the need to obtain, produce, and disseminate foreign-intelligence information, or to retain and disseminate evidence of a crime. 50 U.S.C. §§ 1801(h)(1), (3), 1821(4)(A), (C), 1881a(e)(1).

[CLASSIFIED MATERIAL REDACTED]

D. [CLASSFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

1. Relevant Facts

a. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

b. **[CLASSIFIED MATERIAL REDACTED]**

[CLASSIFIED MATERIAL REDACTED]

c. **[CLASSIFIED MATERIAL REDACTED]**

[CLASSIFIED MATERIAL REDACTED]

d. **[CLASSIFIED MATERIAL REDACTED]**

[CLASSIFIED MATERIAL REDACTED]

e. **[CLASSIFIED MATERIAL REDACTED]**

[CLASSIFIED MATERIAL REDACTED]

f. **[CLASSIFIED MATERIAL REDACTED]**

[CLASSIFIED MATERIAL REDACTED]

g. **[CLASSIFIED MATERIAL REDACTED]**

[CLASSIFIED MATERIAL REDACTED]

2. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

a. **[CLASSIFIED MATERIAL REDACTED]**

[CLASSIFIED MATERIAL REDACTED]

b. **[CLASSIFIED MATERIAL REDACTED]**

[CLASSIFIED MATERIAL REDACTED]

c. **[CLASSIFIED MATERIAL REDACTED]**

[CLASSIFIED MATERIAL REDACTED]

d. **[CLASSIFIED MATERIAL REDACTED]**

[CLASSIFIED MATERIAL REDACTED]

3. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

a. **[CLASSIFIED MATERIAL REDACTED]**

[CLASSIFIED MATERIAL REDACTED]

b. **[CLASSIFIED MATERIAL REDACTED]**

[CLASSIFIED MATERIAL REDACTED]

c. **[CLASSIFIED MATERIAL REDACTED]**

[CLASSIFIED MATERIAL REDACTED]

d. **[CLASSIFIED MATERIAL REDACTED]**

[CLASSIFIED MATERIAL REDACTED]

4. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

a. **[CLASSIFIED MATERIAL REDACTED]**

[CLASSIFIED MATERIAL REDACTED]

b. **[CLASSIFIED MATERIAL REDACTED]**

[CLASSIFIED MATERIAL REDACTED]

5. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

a. **[CLASSIFIED MATERIAL REDACTED]**

[CLASSIFIED MATERIAL REDACTED]

b. **[CLASSIFIED MATERIAL REDACTED]**

[CLASSIFIED MATERIAL REDACTED]

c. **[CLASSIFIED MATERIAL REDACTED]**

[CLASSIFIED MATERIAL REDACTED]

6. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

VI. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

A. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

B. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

1. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

a. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

b. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

c. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

2. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

C. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

1. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

2. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

3. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

D. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

E. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

1. Legal Standard

[CLASSIFIED MATERIAL REDACTED]

2. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

3. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

4. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

5. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

6. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

7. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

8. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

F. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

G. CONCLUSION

[CLASSIFIED MATERIAL REDACTED]

VII. DEFENDANT'S DISCOVERY MOTION SHOULD BE DENIED

Defendant renews (Def.'s Mem., p. 47) his previously-filed motion for "full discovery" of the classified materials relating to the authorization and conduct of the Section 702 collection from which evidence in this case was denied. For the reasons set forth below and in the government's original response to defendant's discovery motion, defendant's request for discovery of classified material should be denied.

A. FISA PROVISIONS GOVERNING REVIEW AND DISCLOSURE

FISA provides that, where the Attorney General certifies that "disclosure [of FISA materials] or an adversary hearing would harm the national security of the United States," a district court "shall, notwithstanding any other law, . . . review *in camera* and *ex parte* the application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted." 50 U.S.C. § 1806(f). This same procedure applies to motions related to Section 702 collection, which is deemed to be Title I FISA electronic surveillance for purposes of such motions. 50 U.S.C. § 1881e(a). If the Attorney General files such a declaration, as he has done here, the district court must review the FISA materials *ex parte* and *in camera* and may disclose the applications and orders (or portions thereof) "only where such disclosure is *necessary* to make an accurate determination of the legality of the surveillance [or search]." 50 U.S.C. § 1806(f) (emphasis added).

Accordingly, FISA requires the court to examine the applications, orders, and related materials *ex parte* and *in camera* to determine the lawfulness of the Section 702 collection. *Id.* If the court is able to assess the legality of the FISA collection by reviewing the government's submissions (and any supplemental materials that the court may request) *in camera* and *ex parte*, it must deny a request for disclosure to the defense. *See, e.g., United States v. El-Mezain*, 664 F.3d 467, 565 (5th Cir. 2011); *United States v. Abu-Jihaad*, 630 F.3d 102, 129 (2d Cir. 2010); *United States v. Damrah*, 412 F.3d 618, 624 (6th Cir. 2005); *United States v. Squillacote*, 221 F.3d 542 (4th Cir. 2000); *United States v. Badia*, 827 F.2d 1458, 1464 (11th Cir. 1987); *United States v. Belfield*, 692 F.2d 141, 147 (D.C. Cir. 1982). A court may order disclosure only if it finds itself incapable of accurately resolving the lawfulness of the FISA collection. *El-Mezain*, 664 F.3d at 567; *Abu-Jihaad*, 630 F.3d at 129.

B. *IN CAMERA, EX PARTE* REVIEW OF FISA MATERIALS IS THE RULE

In light of these requirements, courts consistently have held that "[d]isclosure of FISA materials is the exception and *ex parte*, *in camera* determination is the rule." *El-Mezain*, 664 F.3d at 567 (citing *Abu-Jihaad*, 630 F.3d at 129); *United States v. Duggan*, 743 F.2d 59, 78 (2d Cir. 1984) (same); *United States v. Rosen*, 447 F. Supp. 2d 538, 546 (E.D. Va. 2006). Whenever possible, "the court should proceed *in camera* and without disclosure [of national security information] to determine the legality of a surveillance" in order to avoid frustrating the system designed by Congress to protect the "delicate and sensitive [process of] foreign intelligence gathering" to the greatest degree possible "compatible with the assurance that no injustice is done to a criminal defendant." *Belfield*, 692 F.2d at 149 (internal quotation marks omitted); *see also In re Grand Jury Proceedings of Special April 2002 Grand Jury*, 347 F.3d 197, 203 (7th Cir. 2003) (noting that a case in which "disclosure is necessary" is "one-in-a-million"); Kris &

Wilson, *National Security Investigations* § 29:3 n.1 (2d ed. 2012) ("Necessary means "essential or "required," and therefore the plain language of that provision makes clear that a court may not disclose . . . unless it cannot determine whether the surveillance was unlawful without the assistance of defense counsel and an adversary hearing.").

Until recently, every court to have addressed a motion to disclose FISA applications and orders or to suppress FISA information has been able to determine the legality of the challenged FISA collection based on an *in camera, ex parte* review. *See, e.g., El-Mezain*, 664 F.3d at 566 (quoting district court's statement that no court has ever held an adversarial hearing to assist the court); *but see United States v. Daoud*, No. 12-cr-723, 2014 WL 321384 (N.D. Ill. Jan. 29, 2014) (unpublished) (granting motion for disclosure of FISA materials to defense counsel with security clearance).[49] Even where defendants have alleged specific errors or misrepresentations in the FISA applications, based on their analysis of the evidence in the case, courts have deemed disclosure unnecessary because they were able to adjudicate the surveillance in light of the alleged errors through *in camera, ex parte* review. *See, e.g., El-Mezain*, 664 F.3d at 566; *Abu-Jihaad*, 630 F.3d at 130; *Rosen*, 447 F. Supp. 2d at 552 (denying disclosure despite minimization errors that were inadvertent, disclosed to the FISC, and promptly rectified). Accordingly, if this Court is able to determine the legality of the Section 702 collection from which certain of the evidence in this case was derived based on its *ex parte*, *in camera* review of the government's submission, then there will be no legal basis to disclose any portion of such submission.

/ / /

/ / /

/ / /

[49] The government appealed the district court's order in *Daoud*, and the district court stayed its order pending appeal.

C. DEFENSE PARTICIPATION IS NOT NECESSARY FOR THIS COURT'S REVIEW

Under these standards, the legality of the Section 702 collection at issue in this case may be determined without the need to compel disclosure of classified materials to the defense. As the government's submissions make clear, the Section 702 collection was lawful and the defendant's allegations to the contrary may be considered, and rejected, based on an examination of the classified record. Contrary to defendant's contention, the classified record presents none of the issues that may warrant disclosure, such as "indications of possible misrepresentation of fact, vague identification of the persons to be surveilled, or surveillance records which include a significant amount of nonforeign intelligence information, or any other factors that would indicate a need for disclosure in this case." *United States v. Ott*, 827 F.2d 473, 476 (9th Cir. 1987).

D. DEFENDANT'S ARGUMENTS IN SUPPORT OF DISCLOSURE CONTRAVENE FISA'S STANDARDS AND OTHERWISE LACK MERIT

The government's response to defendant's discovery motion addresses defendant's arguments in support of disclosure. *See* ECF 491 at 15-24. As explained in the government's response and summarized below, defendant's arguments lack merit because they are contrary to the standard set forth in FISA.

Defendant contends (Def.'s Discovery Mem., p. 31), in reliance on various authorized and unauthorized disclosures of information related to Section 702 collection, that the government has no further interest in protecting the classified materials at issue here. However, as set forth in the unclassified Declaration and Claim of Privilege of the Attorney General of the United States, attached hereto as Exhibit 1 and the classified declarations in support thereof, the Executive Branch has determined that disclosure of the materials would harm the national

security of the United States. FISA does not authorize district courts to second-guess the Executive Branch's judgment that disclosure would harm national security. Those judgments, appropriately entrusted to the Executive Branch, "are decisions of a kind for which the Judiciary has neither aptitude, facilities, nor responsibility." *Chicago & S. Airlines, Inc. v. Waterman S.S. Corp.*, 333 U.S. 103, 111 (1948). A district court judge has "little or no background in the delicate business of intelligence gathering," leaving it ill-equipped to understand the significance of disclosing sensitive information and the repercussions for intelligence gathering and United States foreign policy. *C.I.A. v. Sims*, 471 U.S. 159, 176 (1985); *see also id.* at 180 ("[I]t is the responsibility of the Director of Central Intelligence, not that of the judiciary, to weigh the variety of complex and subtle factors in determining whether disclosure of information may lead to an unacceptable risk of compromising the Agency's intelligence-gathering process"); *United States v. Yunis,* 867 F.2d 617, 623 (D.C. Cir. 1989) ("Things that did not make sense to the District Judge would make all too much sense to a foreign counter-intelligence specialist who could learn much about this nation's intelligence-gathering capabilities from what these documents revealed about sources and methods."). In light of these concerns, FISA envisions an inquiry more limited and suitable for a non-specialist court: an *ex parte*, *in camera* review to determine whether the Section 702 collection at issue was lawful.

Defendant contends (Def.'s Discovery Reply, p. 20; *see also* Def.'s Discovery Mem., pp. 33-35)) that the Court should grant disclosure because "the issues presented by the FAA are novel, complex, previously unreviewed by district or appellate courts, and . . . highly controversial."[50] Those arguments provide no basis for disclosure under the applicable standard.

[50] In asserting the lack of any helpful precedent, defendant again fails to mention the decision of the FISA Court of Review in *In re Directives*. Moreover, defendant's assertion that "[t]here was, of course, no informed advocate in place to challenge the government's interpretation and

An order granting disclosure based simply on the assertion that a FISA claim raises complex issues that have not previously been adjudicated would be inconsistent with the statutory scheme. At the time FISA was enacted, every FISA suppression motion would have raised novel issues, yet Congress mandated that FISA litigation be handled *ex parte,* and *in camera*, with disclosure being the exception. Courts have been following that procedure for decades. *E.g., El-Mezain*, 664 F.3d at 567; *Abu-Jihaad*, 630 F.3d at 129; *In re Grand Jury Proceedings*, 347 F.3d at 203; *Duggan*, 743 F.2d at 78. Moreover, the statute requires that courts review the FISA applications and orders *in camera* and *ex parte* first, before even contemplating disclosure. A court's decision to disclose should arise from that review, rooted in facts from the FISA materials, and not from a defendant's contention that the issues he raises are novel and complex.

In *Belfield,* the D.C. Circuit squarely rejected an attempt to compel disclosure on similar grounds. In that case, the defendants asserted that "[q]uestions as to the legality of surveillance conducted under FISA are far too complex to be determined without disclosure and adversary proceedings." 692 F.2d at 147. However, the court recognized that an argument relying on the general complexity of FISA issues would apply in every case, and therefore disclosure would always be "necessary." *Id.* That view, the Court declared, "cannot be correct" because "[t]he language of section 1806(f) clearly anticipates that an *ex parte*, *in camera* determination is to be the rule. Disclosure and an adversary hearing are the exception, occurring *only* when necessary." *Id.* (emphasis in original). Thus, defendant's argument that the alleged novelty and complexity

/ / /

---

application of the FAA before the FISC" ignores that *In re Directives* was not litigated *ex parte*. The FISA Court of Review considered briefing and oral argument from both the government and the communications provider that challenged the directives. *In re Directives*, 551 F.3d at 1008.

of his motion requires disclosure conflicts with *Belfield*, the clear statutory standard governing disclosure, and the process set forth in FISA for review of FISA suppression claims.

Defendant further relies (Def.'s Discovery Mem., pp. 31-33) on the advantages of adversarial procedures that our justice system generally recognizes. Again, however, that argument is contrary to Congress's judgment, embodied in FISA's text, that courts are to review FISA applications and orders *ex parte* and *in camera* except in unusual circumstances. Defendant's reliance on policy judgments are unavailing because they run counter to the policy judgment Congress made in devising FISA's suppression procedures. The advantages of the adversary process were not lost on Congress, but Congress weighed those benefits against the exceptional costs of revealing "sensitive foreign intelligence information." Senate Report at 57; *see also Belfield*, 692 F.2d at 148 (noting that Congress was "aware" of the difficulties of *ex parte* procedures, but that Congress made a "thoroughly reasonable attempt to balance the competing concerns of individual privacy and foreign intelligence."). If a defendant could obtain disclosure merely by pointing out that adversary procedures are generally beneficial and that such procedures would help him formulate his arguments more effectively, disclosure would become the norm, circumventing Congress's intentions and upsetting decades of case law. *See Belfield*, 692 F.2d at 146-48 (noting that Congress "was adamant" that the "carefully drawn procedures" of § 1806(f) were not to be "bypassed by the inventive litigant using a new . . . judicial construction") (citing Senate Report at 63).

Finally, defendant contends (Def.'s Discovery Mem., pp. 36-43) that alleged government misrepresentations in various other national security-related cases support ordering disclosure based on "possible misrepresentations of fact, vague identification of the persons to be surveilled, or surveillance records which include a significant amount of non-foreign intelligence

information." However, defendant fails to recognize that, to justify disclosure, the court must first find that those factors are present with respect to the collection at issue in a particular case, after *ex parte*, *in camera* review. *See Ott*, 827 F.2d at 476 (noting that there are "no indications of possible misrepresentation of fact, vague identification of the persons to be surveilled, or surveillance records which include a significant amount of non-foreign intelligence information, or any other factors that would indicate a need for disclosure in *this case*) (internal quotation marks omitted) (emphasis added); *United States v. Warsame*, 547 F. Supp. 2d 982, 987-88 (D. Minn. 2008) (noting that defendant's allegations that "the government has included misstatements and critical omissions in other FISA applications not at issue here cannot justify disclosure in this case"). As this Court's review of the classified record will show, there is no basis for a finding of material misrepresentations or other factors that would indicate a need for disclosure in this case.

VIII. DEFENDANT IS NOT ENTITLED TO A HEARING UNDER *FRANKS V. DELAWARE*

Defendant has renewed his request for a *Franks* hearing relating to the Title I and III FISA applications that were the subject of his pre-trial FISA suppression motion. (Def.'s Mem. 44-47). As explained below, there is no basis for the Court to conduct a *Franks* hearing.

When a defendant makes the requisite showing, the Court may conduct a *Franks* hearing to determine if there are material misrepresentations of fact, or omissions of material fact, in the FISA applications sufficient to warrant suppression of evidence obtained or derived from Title I and Title III FISA collections. *See Franks v. Delaware*, 438 U.S. 154, 171 (1978); *United States v. Ning Wen,* 477 F.3d 896, 897 (7th Cir. 2007). To merit a *Franks* hearing, the defendant first must make a "concrete and substantial preliminary showing" that: (1) the affiant deliberately or

recklessly included false statements, or failed to include material information, in the affidavit; and (2) the misrepresentation was essential to the finding of probable cause. *Franks*, 438 U.S. at 155-56; *United States v. Colkley*, 899 F.2d 297, 301 (4th Cir. 1990); *United States v. Duggan*, 743 F.2d 59, 77 n.6; *United States v. Kashmiri,* 2010 WL 4705159, *5 (N.D. Ill. 2010) (defendant "has not made any showing – let alone a substantial one – that an Executive Branch officer knowingly and intentionally, or recklessly, included a false statement in the FISA application [and w]ithout such a showing, he is foreclosed from obtaining a hearing"). Failure of the defendant "to satisfy either of these two prongs proves fatal to a *Franks* hearing." *Id.* at *5; *United States v. Mubayyid*, 521 F. Supp. 2d 125, 130-31 (D. Mass. 2007).

The defendant's burden in establishing the need for a *Franks* hearing is a heavy one. *United States v. Jeffus*, 22 F.3d 554, 558 (4th Cir. 1994). The defendant must submit allegations of deliberate falsehood or of reckless disregard for the truth, accompanied by an offer of proof. *Franks*, 438 U.S. at 171. Allegations of negligence or innocent mistake are insufficient, *id.,* as are allegations of insignificant or immaterial misrepresentations or omissions. *Colkley*, 899 F. 2d at 301-02. Moreover, contrary to defendant's contention (*see* Def.'s Mem., p. 45), a defendant's lack of access to the FISA applications and orders is not an adequate substitute for the required showing. Although this situation presents a quandary for defense counsel when FISA-derived evidence comes into play, Congress and the courts have recognized that such difficulty does not justify the disclosure of FISA materials:

> We appreciate the difficulties of appellants' counsel in this case. They must argue that the determination of legality is so complex that an adversary hearing with full access to relevant materials is necessary. But without access to the relevant materials their claim of complexity can be given no concreteness. It is pure assertion.
>
> Congress was also aware of these difficulties. But it chose to resolve them through means other than mandatory disclosure. In FISA Congress has made a

> thoroughly reasonable attempt to balance the competing concerns of individual privacy and foreign intelligence . . . . Appellants are understandably reluctant to be excluded from the process whereby the legality of a surveillance by which they were incidentally affected is judged. But it cannot be said that this exclusion rises to the level of a constitutional violation.

United States v. Belfield, 692 F.2d 141, 148 (D.C. Cir 1982); *see also Kashmiri,* 2010 WL 4705159, at *6:

> Nevertheless, to challenge the veracity of the FISA application, Defendant must offer substantial proof that the FISC relied on an intentional or reckless misrepresentation by the government to grant the FISA order. The quest to satisfy the *Franks* requirements might feel like a wild-goose chase, as Defendant lacks access to the materials that would provide this proof. This perceived practical impossibility to obtain a hearing, however, does not constitute a legal impossibility.

Defendant cannot show that material misrepresentations or omissions of material fact regarding Section 702 collection were deliberately or recklessly made to the FISC because there were none. To the contrary, the relevant information regarding the prior Section 702 collection was made available to the FISC and the Court.

[CLASSIFIED MATERIAL REDACTED]

Defendant also alleges that "the government's recent conduct in terms of candor to the court in federal cases involving national security issues" provides the basis for a *Franks* hearing. (Def.'s Mem., p. 46). Such allegations cannot establish that the particular FISA applications at issue in this case include material misstatements that were deliberately or recklessly made, or that they contain material omissions, nor can such allegations establish that there were errors of that type that were essential to the FISC's probable cause findings.

Other courts have rejected similar attempts by defendants to force a *Franks* hearing challenging the validity of FISA orders based on speculation. *See Kashmiri,* 2010 WL 4705159, at *6 (noting that the court "has already undertaken a process akin to a *Franks* hearing through

its *ex parte, in camera* review"); *United States v. Abu-Jihaad*, 531 F.Supp.2d 299, 310 (D.Conn. 2008), *aff'd* 630 F.3d 102 (2d Cir. 2010)); *United States v. Hassoun*, No. 04-CR-60001, 2007 WL 1068127, at *4 (S.D. Fla. Apr. 4, 2007); *Mubayyid,* 521 F. Supp. 2d at 130-31. This Court likewise should reject defendant's attempt to hold a *Franks* hearing in this case without making the proper showing.

IX. DEFENDANT IS NOT ENTITLED TO SUPPRESSION OF ANY EVIDENCE BASED ON COLLECTION OF TELEPHONY METADATA PURSUANT TO SECTION 215 OF THE PATRIOT ACT

Defendant has moved for suppression of all fruits of additional alleged surveillance programs he believes likely were used in the government's investigation of him. He also argues that the Court should address the lawfulness of the telephony metadata program, which is conducted pursuant to Section 215 of the Patriot Act (codified at 50 U.S.C. § 1861) and which defendant believes likely was used to collect his telephony metadata. (Def.'s Mem., pp. 40-41). Defendant's arguments are meritless. There is no reason for the Court to address the lawfulness of this program, and defendant is not entitled to suppression of any evidence based on the collection of telephony metadata pursuant to Section 215 of the Patriot Act or any other surveillance activities defendant alleges occurred.

[CLASSIFIED MATERIAL REDACTED]

///

///

///

///

///

///

X. CONCLUSION

Based on the above discussion and analysis, the government requests that the Court deny defendant's Alternative Motion for Suppression of Evidence and a New Trial Based on the Government's Introduction of Evidence at Trial and Other Uses of Information Derived from Unlawful Electronic Surveillance and his Motion for Full Discovery Regarding the Facts and Circumstances Underlying Surveillance.

Respectfully submitted this 2nd day of May 2014.

S. AMANDA MARSHALL
United States Attorney

s/ Ethan D. Knight
ETHAN D. KNIGHT, OSB #99298
PAMALA R. HOLSINGER, OSB #89263
Assistant United States Attorneys
(503) 727-1000

JOHN P. CARLIN
Assistant Attorney General
for National Security

GEORGE Z. TOSCAS
J. BRADFORD WIEGMANN
TASHINA GAUHAR
Deputy Assistant Attorneys General
National Security Division

JOLIE F. ZIMMERMAN, DCB #465110
Trial Attorney
Counterterrorism Section
National Security Division
United States Department of Justice

UNITED STATES DISTRICT COURT
DISTRICT OF OREGON

UNITED STATES OF AMERICA, Plaintiff, v. MOHAMED OSMAN MOHAMUD, Defendant.	)	No. 10-CR-475-KI DECLARATION AND CLAIM OF PRIVILEGE

DECLARATION AND CLAIM OF PRIVILEGE
OF THE ATTORNEY GENERAL OF THE UNITED STATES

I, Eric H. Holder, Jr., hereby declare the following:

1. I am the Attorney General of the United States of America and head of the United States Department of Justice, an Executive Department of the United States. I have official custody of and control over the files and records of the United States Department of Justice. The matters stated herein are based on my knowledge, on consideration of information available to me in my official capacity as Attorney General, on discussions that I have had with other Justice Department officials, and on conclusions I have reached after my review of this information.

2. Under the authority of 50 U.S.C. §§ 1806(f), 1825(g), and 1881e(a), I submit this declaration pursuant to the Foreign Intelligence Surveillance Act of 1978 ("FISA"), as amended, in connection with the above-captioned criminal proceeding. I have been advised that the Government used information derived from electronic surveillance, physical searches, and the targeting of non-U.S. persons outside the United States, all conducted pursuant to FISA, in the criminal proceeding against the Defendant. *See* 50 U.S.C. §§ 1806(c), 1825(d), and 1881e(a).

Accordingly, the Defendant, by and through his attorney, has filed motions seeking disclosure and suppression of FISA-related materials (hereinafter the "Defendant's Motions"). The Government will file an opposition to the Defendant's Motions. For the reasons set forth in the Government's Opposition, it is necessary to provide this Court with the applications and certifications submitted to, and the orders issued by, the Foreign Intelligence Surveillance Court ("FISC"), as well as other related documents (hereinafter collectively referred to as "the FISA Materials").

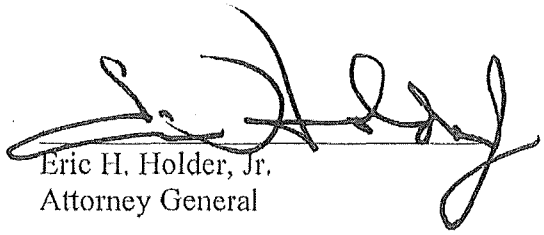
3. Based on the facts and considerations set forth below, I hereby claim that it would harm the national security of the United States to disclose or hold an adversarial hearing with respect to the FISA Materials. The United States will submit the relevant classified documents to this Court as part of a "Sealed Appendix," so this Court may conduct an *in camera*, *ex parte* review of the legality of the FISA collection at issue. My Claim of Privilege also extends to the classified portions of any memoranda and briefs the Government may file in connection with this litigation and to any oral representations that may be made by the Government that reference the classified information contained in the FISA Materials.

4. In support of my Claim of Privilege, the United States is submitting to the Court for *in camera, ex parte* review the Declarations of James R. Clapper, Director of National Intelligence, and John Giacalone, Assistant Director, Counterterrorism Division, Federal Bureau of Investigation. The Declarations of Mr. Clapper and Mr. Giacalone set forth, in detail, the specific facts on which my Claim of Privilege is based. The Declarations of Mr. Clapper and Mr. Giacalone are classified at the "TOP SECRET" level.

5. Relying on the facts set forth in the Declarations of Mr. Clapper and Mr. Giacalone, I certify that the unauthorized disclosure of the FISA Materials that are classified at the "TOP SECRET" level could reasonably be expected to cause exceptionally grave damage to the national security of the United States. I further certify that the unauthorized disclosure of the FISA materials that are classified at the "SECRET" level reasonably could be expected to cause serious damage to the national security of the United States. The FISA Materials contain sensitive and classified information concerning United States intelligence sources and methods and other information related to efforts of the United States to conduct counterterrorism investigations, including the manner and means by which those investigations are conducted. As a result, the unauthorized disclosure of the information could harm the national security interests of the United States.

6. I respectfully request that the Court treat the contents of the Sealed Appendix, for security purposes, in the same sensitive manner that the contents were treated in the submission to this Court, and to return the Sealed Appendix to the Department of Justice upon the disposition of the Defendant's Motions. The Department of Justice will retain the Sealed Appendix under the seal of the Court subject to any further orders of this Court or other courts of competent jurisdiction.

Pursuant to Title 28, United States Code, Section 1746, I declare under penalty of perjury that the foregoing is true and correct. Executed on May 2, 2014.



Eric H. Holder, Jr.
Attorney General