IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO

UNITED STATES OF AMERICA, Plaintiff, v. 1. JAMSHID MUHTOROV, and 2. BAKHTIYOR JUMAEV, Defendants.	Case No.: 12-CR-00033-JLK

GOVERNMENT'S UNCLASSIFIED MEMORANDUM IN OPPOSITION TO DEFENDANTS' MOTION TO SUPPRESS EVIDENCE OBTAINED OR DERIVED FROM SURVEILLANCE UNDER THE FISA AMENDMENTS ACT AND MOTION FOR DISCOVERY

TABLE OF CONTENTS

I. INTRODUCTION

A. OVERVIEW

[1]The government is filing this unclassified memorandum in opposition to: (1) Defendant Jamshid Muhtorov's ("Muhtorov") "Motion to Suppress Evidence Obtained or Derived from Surveillance Under the FISA Amendments Act and Motion for Discovery," which was joined by Defendant Bakhtiyor Jumaev ("Jumaev") ("defendants' motion") (CR 520; CR 521). In essence, the defendants' motion seeks: (1) disclosure of records and documents relating to, among other things, the government's acquisition, use, and dissemination of either defendants' communications acquired pursuant to Section 702 of the FISA Amendments Act of 2008 ("FAA") (collectively, "the Section 702 materials"); and (2) suppression of all evidence obtained or derived from surveillance conducted pursuant to the FAA. For the reasons set forth below, the Court should deny the defendants' motion in its entirety.

The defendants' motion for discovery and suppression was filed in response to the government's Second FISA Notice as to Muhtorov, filed on October 25, 2013, which provided "notice to defendant and the Court, pursuant to 50 U.S.C. §§ 1806(c) and 1881e(a), that the 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 Second Notice," CR 457). The Government's Second Notice was filed based on a recent determination by the government that certain evidence referenced in the original FISA notification, filed on February 7, 2012 (CR 12), obtained or derived from collection conducted pursuant to Title I and Title III of FISA, was itself also derived from Title VII collection

[1] **CLASSIFIED MATERIAL REDACTED**

as to which defendant Muhtorov 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. Defendants seek suppression of the Section 702-derived evidence used in this case, as well as discovery of the FISA materials.[2]

The defendants' motion has triggered this Court's review of the relevant Section 702 materials pursuant to 50 U.S.C. §§ 1881e(a) and 1806(f) to determine whether the Section 702 intelligence collection at issue herein was lawfully authorized and conducted in accordance with the requirements of the FAA. In particular, Section 1806(f) provides that, where the Attorney General certifies that "disclosure 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); *see also* 50 U.S.C. § 1825(g). This same procedure applies to motions to disclose Section 702-related materials or to suppress information obtained or derived from Section

[2] The defendants' suggestion that some bad faith or bad purpose underlies this determination is unfounded. Defs. Mot. 5-7. The Department has always understood that it is required to notify any "aggrieved person" of its intent to use or disclose, in a proceeding against such person, any information obtained or derived from Title VII collection as to which that person is an aggrieved person, in accordance with 50 U.S.C. §§ 1806(e), and 1881e(a). Prior to recent months, however, the Department had not considered the particular question of whether and under what circumstances information obtained through electronic surveillance under Title I or physical search under Title III could also be considered to be derived from prior collection under Title VII. After conducting a review of the issue, the Department determined that information obtained or derived from Title I or Title III FISA collection may, in particular cases, also be derived from prior Title VII collection, such that notice concerning both Title I/III and Title VII collections should be given in appropriate cases with respect to the same information. The Second Notice filed in this case, which the government filed based on its own review, resulted from that determination and demonstrates good faith, not misconduct.

702 acquisitions, which is deemed to be electronic surveillance conducted 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.[3]

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 defendants' motion, in accordance with the provisions of 50 U.S.C. §§ 1881e(a) and 1806(f). *See also* 50 U.S.C. § 1825(g).

The government expects that the Court will conclude from its *in camera, ex parte* review that: (1) defendant Jumaev lacks standing to challenge the FAA in this case; (2) the acquisition, retention, and dissemination of foreign intelligence information pursuant to the FAA at issue herein was lawfully authorized and conducted in accordance with the Act; (3) the FAA complies with the Fourth Amendment and Article III of the U.S. Constitution; (4) evidence obtained or derived from the FAA collection at issue herein should not be suppressed; and (5) the defendants' discovery requests should be denied to the extent that they seek disclosure of materials related to the FAA.

CLASSIFIED MATERIAL REDACTED

In opposition to the defendants' 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.[4]

---

[3] The Declaration and Claim of Privilege of the Attorney General of the United States is being filed both publicly and as part of this classified filing. *See* Sealed Exhibit 1.

CLASSIFIED MATERIAL REDACTED

B. SUMMARY OF THE ARGUMENT

In subsequent sections of this Memorandum, the government will: (1) present an overview of the case facts, background, procedural history, and summary of the collection at issue; (2) give an overview of Section 702 of the FAA; (3) describe the Section 702 certification(s) and summarize the collection at issue in this case; (4) establish defendant Jumaev's lack of standing to challenge the constitutionality of Section 702 or the Section 702 collection at issue in this case; (5) establish the constitutionality of Section 702 as applied in this case; (6) establish that the specific Section 702 collection at issue in this case was legally authorized and conducted pursuant to the applicable targeting and minimization procedures; (7) explain why defendants' motion for discovery of the Section 702 materials should be denied; and (8) explain why defendants are not entitled to a hearing under *Franks v. Delaware*, 438 U.S. 154 (1978).

All of the government's pleadings and supporting materials are being submitted not only to oppose the defendants' motion but also to support the United States' request, pursuant to FISA, that this Court (1) conduct an *in camera, ex parte* review of the Section 702 materials; (2) find that the Section 702 acquisition was lawfully authorized and conducted in conformity with the Constitution, the statute, and the approved targeting and minimization procedures; (3) hold that disclosure to the defense of the Section 702 materials and the government's classified submissions is not required because the Court is able to make an accurate determination of the legality of the collections at issue without disclosing any portion thereof; and (4) order that none of the Section 702 materials be disclosed to the defense, and instead that they be maintained by the United States under seal.

---

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

1. Defendant Jumaev's Motion Should be Summarily Denied

Because the government is not entering into evidence or otherwise using or disclosing information obtained or derived from Section 702 collection to which Jumaev is aggrieved in this prosecution, he has no standing to challenge the constitutionality of Section 702 or the Section 702 collection at issue in this case. 50 U.S.C. § 1806(d); *see* 50 U.S.C. § 1825(d); *see also* 50 U.S.C. § 1881e(a). *See infra* Part II.

2. Section 702 Is Constitutional

In their motion to suppress evidence derived from Section 702 foreign intelligence acquisition, defendants argue that Section 702 of the FAA violates the Fourth Amendment and Article III of the United States Constitution. As an initial matter, 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. *See In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act*, 551 F.3d 1004, 1010 (FISA 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"). As applied to the acquisition at issue here, Section 702 is constitutional. *See infra* at Part III.

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 III.A.

Second, Section 702, in requiring the Foreign Intelligence Surveillance Court (FISC) to review the government's proposed certification(s) 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 III.B.

3. The Collection In this Case Was Lawfully Authorized and Conducted

In addition to challenging the general constitutionality of Section 702, the defendants also question 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 certification(s) 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 certification(s) and procedures. *See infra* at Part IV.A-C.

CLASSIFIED MATERIAL REDACTED

4. Defendants' 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 disclose classified materials to the defense. As the government's submissions make clear, the Section 702 collection was lawful and the defendants' allegations to the contrary may be considered, and rejected, based on an examination of the classified record. Contrary to the defendants' 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. Nor are the Section 702 materials exculpatory or otherwise subject to disclosure under *Brady v. Maryland*, 373 U.S. 83 (1963). *See infra* at Part V.

5. No *Franks* Hearing Should Be Held

Finally, defendants are not entitled to a hearing under *Franks*, 438 U.S. at 154, because there were no material omissions or misrepresentations of fact. Moreover, defendants' 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. *See infra* Part VI.

C. BACKGROUND

1. The FBI's Investigation of the Defendants

CLASSIFIED MATERIAL REDACTED

2. Procedural History

On January 19, 2012, the government charged Muhtorov by criminal complaint in the District of Colorado with providing material support or resources to a designated FTO, namely, the IJU, in violation of 18 U.S.C. § 2339B. (CR 1). On January 23, 2012, a federal grand jury sitting in the District of Colorado returned a one-count indictment charging Muhtorov with the same offense.

(CR 5). On March 20, 2012, the grand jury returned a superseding indictment charging Muhtorov with two counts of providing and attempting to provide material support and resources to the IJU, and charging Muhtorov and Jumaev with one count of providing and attempting to provide material support and resources to the IJU, and one count of conspiring to commit that offense, all in violation of 18 U.S.C. § 2339B. (CR 50). The grand jury returned a second superseding indictment on March 22, 2012, containing the same charges as those set forth in the first superseding indictment. (CR 59).

On February 7 and April 4, 2012, pursuant to 50 U.S.C. §§ 1806(c) and 1825(d), the United States provided notice to Muhtorov and Jumaev respectively that it intended "to offer into evidence or otherwise use or disclose in any proceedings in the above-captioned matter, information obtained and derived from electronic surveillance or physical search conducted pursuant to the Foreign Intelligence Surveillance Act of 1978 (FISA), as amended, 50 U.S.C. §§ 1801-1811, 1821-1829." (CR 12, 68). The statutes cited in those notices permit electronic surveillance and physical search when a significant purpose is to obtain foreign intelligence information, provided that the government establishes to the satisfaction of the FISC that, among other things, there is probable cause to believe that the target is an agent of a foreign power. *See* 50 U.S.C. §§ 1801, 1804-1805, 1821, 1823-24. Electronic surveillance under these provisions is commonly referred to as Title I collection, while physical search is commonly referred to as Title III collection.

On February 8, 2012, Muhtorov filed a motion to suppress FISA-acquired evidence for purposes of detention (CR 14), and on May 25, 2012, Muhtorov filed a supplemental motion to suppress FISA-acquired evidence. (CR 125). On July 30, 2012, Jumaev filed his combined FISA-related motions. (CR 157). After conducting an *ex parte*, *in camera* review of the relevant material, the Court denied both defendants' FISA-related motions on September 24, 2012. (CR 196).

On October 25, 2013, pursuant to 50 U.S.C. §§ 1806(c) and 1881e(a), the United States provided the Second FISA Notice to Muhtorov, stating that it intended "to offer into evidence or otherwise use or disclose in any proceedings in the above-captioned matter information obtained or derived from acquisition of foreign intelligence information conducted pursuant to the Foreign Intelligence Surveillance Act of 1978 (FISA), as amended, 50 U.S.C. §1881a." (CR 457). On January 29, 2014, Muhtorov filed a motion to suppress evidence obtained or derived from collection under Section 702, together with a motion for discovery of materials related to the Section 702 collection. (CR 520).

The government has not provided similar notice to Jumaev under 50 U.S.C. § 1881a. Jumaev filed a motion requesting that the court order the government to provide him notice as to its intent to use evidence obtained or derived from surveillance authorized by the FAA. (CR 458). In its response and surreply to Jumaev's motion, the government stated that it does not intend to introduce or otherwise use or disclose against Jumaev in any trial, hearing or other proceeding in this case evidence obtained or derived from Section 702 acquisition to which Jumaev is an aggrieved person. Thus, Jumaev is not entitled to any additional notice under FISA. (CR 470, 525). Notwithstanding the fact that he lacks statutory standing to seek suppression of any Section 702-obtained or derived evidence, on January 30, 2014, Jumaev filed a motion to adopt Muhtorov's Section 702-related suppression motion and motion for discovery. (CR 521).

3. Overview of the FAA Collection at Issue

As set forth in the government's submissions in the previous FISA litigation, the government intends to introduce evidence obtained and derived from electronic surveillance and searches that were conducted pursuant to Titles I and III of FISA. This Court has already upheld the legality of that Title I and III collection. (CR 196.) Thus, at issue in defendants' instant motion is the use of

evidence obtained or derived from collection pursuant to Section 702 to which defendant Muhtorov is an aggrieved person.

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

D. OVERVIEW OF FISA AND THE FISA AMENDMENTS ACT

1. 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. Ct*, 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. 604, 95th Cong., 1st Sess. 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. [5]

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; *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,

[5] The judges which sit on the FISC are Article III judges with life tenure that serve by designation of the Chief Justice of the Supreme Court of the United States. 50 U.S.C. § 1803(a).

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. 701, 95th Cong., 2d Sess. 7 & n.2, 34-35 & n.16 (1978).[6] Congress was told in the hearing leading to FISA's enactment that the acquisition of

[6] Executive Order No. 12333, as amended, addresses, *inter alia*, the government's "human and technical collection techniques . . . undertaken abroad." Exec. Order No. 12333, § 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-

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 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 FISA Hrg.").[7] Congress heard similar testimony from other witnesses.[8] 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. 701, 95th Cong. 2d Sess. 71 ("[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

---

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).

[7] 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., 180-81 (1976).

[8] *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. 8 (1976) (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. 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").

surveillance, or wire surveillance of transoceanic cables offshore or on foreign soil, outside the statute's regulatory framework.

2. 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. (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. 209, 110th Cong., 1st Sess. 2-5 (2007). 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. 19 (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.*[9]

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. 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 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. 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

[9] *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).

> 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. (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.[10] The fix 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. 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. No. 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

---

[10] 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.

May 1, 2007 FISA Modernization Hrg. 18.

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. 209, 110th Cong., 1st Sess. 5-6. 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 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).[11] One private party brought such a challenge, and both the FISC and the FISA Court of Review upheld the PAA. *See In re Directives*, 551 F.3d 1004 (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).

[11] 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).

3. Section 702 of the FISA Amendments Act

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.[12] 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).[13] 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 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).[14]

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).

---

[12] 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.

[13] 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.

[14] 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).

> (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.

a. 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).[15]

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 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).[16]

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

---

[15] 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.

[16] **CLASSIFIED MATERIAL REDACTED**

b. The FISC's Order(s)

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

c. 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.*[17]

CLASSIFIED MATERIAL REDACTED

d. 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 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).[18] 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).

---

[17] **CLASSIFIED MATERIAL REDACTED**

[18] 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.

CLASSIFIED MATERIAL REDACTED

1. Targeting Procedures

CLASSIFIED MATERIAL REDACTED

a. **CLASSIFIED MATERIAL REDACTED**

CLASSIFIED MATERIAL REDACTED

b. **CLASSIFIED MATERIAL REDACTED**

CLASSIFIED MATERIAL REDACTED

2. 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 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

e. 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.").[19]

f. 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.

---

[19] Rule 13(b) of the Rules of Procedures for the FISC requires the government to report, in writing, all instances of non-compliance. FISC R. P. 13b(1) The government reports Section 702 compliance incidents to the FISC via individual notices and quarterly reports. *See* 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.

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).[20] 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 "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).[21] 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).

---

[20] 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).

[21] 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).

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.*

II. DEFENDANT JUMAEV'S MOTION SHOULD BE DENIED

The government's notice obligations regarding its use of FISA information under §§ 1806(c), 1825(d), and 1881e apply only if the government (1) "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(d); *see* 50 U.S.C. § 1825(d); *see also* 50 U.S.C. § 1881e(a). With regard to electronic surveillance, an aggrieved person is "a person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance." 50 U.S.C. § 1801(k).

CLASSIFIED MATERIAL REDACTED

III. DEFENDANTS' CONSTITUTIONAL ARGUMENTS LACK MERIT

Defendants move for suppression of evidence derived from the acquisition of foreign intelligence information under Section 702 on the ground that Section 702 is unconstitutional. (Defs. Mot. 21-47). For the reasons set forth below, defendants' motion should be denied.

A. THE ACQUISITION 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 certification(s) 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 at 1010-11.

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, if not completely eliminated, 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) 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. 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.[22] For that

[22] 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 702 (based on the

reason, to the extent defendants attempt a facial challenge to Section 702 (*see* Defs. Mot. 49 n.15), the challenge fails, because the statute is constitutional in its application to persons unprotected by the Fourth Amendment. *See United States v. Salerno*, 481 U.S. 739, 745 (1987) (noting that, outside of the First Amendment context, a statute is facially invalid only if it is unconstitutional in all of its possible applications).[23]

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

The statute does not permit United States persons to be intentionally targeted under Section 702. To the extent that U.S. person communications are collected *incidentally* under Section 702 in the course of intelligence collection targeted at one or more non-U.S. persons outside the United States: "incidental collections occurring as a result of constitutionally permissible acquisitions do not render those acquisitions unlawful." *In re Directives*, 551 F.3d at 1015; *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); *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. Martin*, 599 F.2d 880, 884-85 (9th Cir. 1979), *overruled in part 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

---

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(1)(3)(A)(iii).

[23] In any event, 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.

conversations of unknown third 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."). Therefore the incidental collection of U.S. person communications was lawful.[24]

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 I.D.3.d.2. *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").

---

[24] **CLASSIFIED MATERIAL REDACTED**

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").[25] Before initiating surveillance of a foreign target, the government cannot know the identities of all those with whom the target will communicate in the future, 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."). Thus, 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

[25] While defendants cite cases recognizing a warrant requirement for electronic surveillance in the domestic context (Defs. Mot. 27, 32), they do 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.

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) Hearing Before the H. Judiciary Comm.*, 110th Cong., 1st Sess. 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 not originally intended to protect "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." *Id.*

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, at *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 certain contexts, a search or surveillance is impermissible without a warrant or other individualized court order. *See Vernonia Sch.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 Sch. 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. 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); *United States v. Buck*, 548 F.2d 871, 875 (9th Cir. 1977) ("Foreign security wiretaps are a recognized exception to the general warrant requirement."); *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");[26] *but see Zweibon v. Mitchell*, 516 F.2d 594, 618-20 (D.C. Cir. 1975) (en

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

banc) (plurality opinion suggesting in dicta that a warrant may be required even in a foreign intelligence investigation).[27] 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, defendants contend (Defs. Mot. 32) 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).

Defendants rely (Defs. Mot. 27-29) 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

[27] 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.

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*, 133 S. Ct. at 1143 (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."). 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 ("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.[28]

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

[28] **CLASSIFIED MATERIAL REDACTED**

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").[29] 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* 154 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 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

[29] **CLASSIFIED MATERIAL REDACTED**

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. Ry. Labor Execs.' 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. *Cf. 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, *see* 50 U.S.C. § 1881a(b), 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).[30]

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.

f. *Truong* Does Not Preclude Application of the Foreign Intelligence Exception to Section 702 Collection

Defendants contend (Defs. Mot. 32-33), relying on *Truong*, that the foreign intelligence exception is limited to circumstances where: (1) the surveillance was directed at a specific foreign agent or foreign power; (2) the *primary* purpose was to gather foreign intelligence information; and

[30] For these reasons, defendants' claim (Defs. Mot. 31-32) that the availability of Title I FISA warrants undermines the rationale for the foreign intelligence exception is incorrect. Moreover, 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 (Oct. 3, 2011).

(3) the surveillance was personally approved by the President or Attorney General. This argument misreads *Truong* and should be rejected.

The specific foreign-agent-or-power limitation was recognized in *Truong*, which involved unilateral Executive Branch surveillance directed at a person within the United States. However, nothing in *Truong* suggests that foreign intelligence surveillance directed at non-U.S. persons outside the United States, as authorized by Congress and conducted pursuant to targeting and minimization procedures approved by the FISC, must be directed only at a specific foreign agent or foreign power. And, for the reasons explained in Part III.A.2.d above, such a requirement would seriously undermine the government's ability to obtain foreign intelligence information in this context and, in any event, would be unnecessary since the targets of the surveillance are persons unprotected by the Fourth Amendment.[31]

Defendants' second limitation invokes the purported "primary purpose" requirement that has been repeatedly rejected by Congress and the courts. *See In re Directives*, 551 F.3d at 1011; *In re Sealed Case*, 310 F.3d at 742-45; *Abu-Jihaad*, 630 F.3d at 121; *Duka*, 671 F.3d at 343-45. As the FISA Court of Review has explained, the "primary purpose" language adopted in *Truong* "drew an unstable, unrealistic, and confusing line between foreign intelligence purposes and criminal investigation purposes." *In re Directives*, 551 F.3d at 1011. Because "[a] surveillance with a foreign intelligence purpose often will have some ancillary criminal-law purpose," such as "apprehension of terrorism suspects," *id.*, attempting to discern whether criminal-law purposes are primary or secondary to intelligence purposes can be an artificial exercise. *See In re Sealed Case*, 310 F.3d at 743. Accordingly, "the more appropriate consideration is the programmatic purpose of the surveillances and whether – as in the special needs cases – that programmatic purpose involves

[31] **CLASSIFIED MATERIAL REDACTED**

some legitimate objective beyond ordinary crime control." *In re Directives*, 551 F.3d at 1011; *see also In re Sealed Case*, 310 F.3d at 745-46. In *In re Sealed Case*, the FISA Court of Review construed the "significant purpose" requirement to preclude the government from using FISA as a "device to investigate wholly unrelated ordinary crimes." *Id.* at 735-36. Congress used the same term in the PAA, and Section 702 should be presumed to have incorporated this construction. *See Cannon v. Univ. of Chic.*, 441 U.S. 677, 696-99 (1979). So construed, the "significant purpose" standard is sufficient for purposes of the "special needs" doctrine and "foreign intelligence" exception. *See Edmond*, 531 U.S. at 40-42 (noting that the doctrine turns on whether the programmatic purpose of a search goes beyond the investigation of "ordinary criminal wrongdoing"); *In re Directives*, 551 F.3d at 1011 (upholding directives under the PAA because "[t]heir stated purpose 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").

As for the third purported limitation defendants invoke, it is true that the Attorney General does not personally approve each individual acquisition under Section 702. However, the Attorney General and Director of National Intelligence play a significant role in establishing and authorizing the certification and procedures that govern the acquisition. *See* 50 U.S.C. 1881a(a) (collection under Section 702 must be jointly authorized by the Attorney General and Director of National Intelligence). In addition, unlike the unilateral executive branch surveillance in *Truong*, Section 702 collection is governed by stringent, court-approved procedural safeguards and extensive oversight by Congress and by the FISC. Those requirements provide sufficient authorization and oversight, by all three branches of government, for purposes of the foreign intelligence exception.

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 III.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." *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). 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, when the search involves modest intrusions on the individual's privacy, and when alternative safeguards restrain the government within reasonable limits. *See, e.g.*, *Ill. 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).

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.[32] 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 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.[33]

---

[32] 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.

[33] *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. 551 F.3d at 1008.

The FAA provisions, certification(s), 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.[34] 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. Defendants' 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 ("The Court found in those prior dockets that the targeting and minimization procedures 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; *Haig v. Agee*, 453 U.S. 280, 307 (1981) ("It is 'obvious and

[34] **CLASSIFIED MATERIAL REDACTED**

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 (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. 645 (II) 112th Cong., 2nd Sess. 3 (Aug. 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.

b. Defendants Have, At Most, Limited Expectations of Privacy in Communications Obtained Through Targeting Non-U.S. Persons Outside the United States

The other side of the Fourth Amendment reasonableness balance is the degree to which the search "intrudes upon an individual's privacy." *Knights*, 534 U.S. at 118-19 (citation omitted). Of course, where an individual has no reasonable expectation of privacy at all, his Fourth Amendment claim fails at the threshold. And where the search takes place in circumstances where the individual's expectations of privacy are limited, the diminished character of the privacy interest must be taken into account in the court's assessment of reasonableness.

An individual's ability to "claim the protection of the Fourth Amendment depends . . . upon whether" he "has a legitimate expectation of privacy in the invaded place." *Rakas v. Illinois*, 439 U.S. 128, 143 (1978).[35] A court may not exclude evidence under the Fourth Amendment unless it finds that an unlawful search or seizure "invaded [the defendant's] legitimate expectation of privacy rather than that of a third party." *United States v. Payner*, 447 U.S. 727, 731 (1980). To claim the protection of the Fourth Amendment, a defendant "must demonstrate that he personally has an expectation of privacy in the place searched, and that his expectation is reasonable; *i.e.*, one that has 'a source outside of the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society.'" *Minnesota v. Carter*, 525 U.S. 83, 88 (1998) (quoting *Rakas*, 439 U.S. at 144 n.12); *see also, e.g., United States v.*

[35] Although the Supreme Court has formerly analyzed questions concerning an individual's ability to claim Fourth Amendment protections under the rubric of "standing," the Court made clear in *Rakas* that "definition of those rights is more properly placed within the purview of substantive Fourth Amendment law than within that of standing." 439 U.S. at 140. Nevertheless, the nomenclature of "standing" is still commonly used by lower courts when addressing whether an individual can assert a Fourth Amendment claim.

Wells, 739 F.3d 511, 522-23 (10th Cir. 2014) (holding that an individual lacked a reasonable expectation of privacy in his communications while in another person's hotel room).

1. Senders of electronic communications do not retain a reasonable expectation of privacy in communications once they arrive at their destination

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 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 a communication, the sender loses any cognizable Fourth Amendment rights with respect to that communication. 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 communication to others, leave the communication freely accessible to others, or that the U.S. government (or a foreign government) will obtain the communication.[36]

This rule applies to physical mail, even within the United States. Although 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

[36] 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.

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. Perrine*, 518 F.3d 1196, 1204-05 (10th Cir. 2008) (noting that an individual "may not . . . enjoy . . . an expectation of privacy in 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).

2. **CLASSIFIED MATERIAL REDACTED**

CLASSIFIED MATERIAL REDACTED

3. **CLASSIFIED MATERIAL REDACTED**

CLASSIFIED MATERIAL REDACTED

4. Any remaining expectation of privacy in the international communications at issue was significantly diminished

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 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 because, at a minimum, privacy expectations are sharply reduced in their context.[37]

[37] Any expectations of privacy defendants may have had in their electronic communications with non-U.S. persons overseas were also diminished by the prospect that their foreign correspondents could be targets 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

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.

1. 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

---

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.

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.

2. 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 ("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 defendants' contention that collection under Section 702 is unreasonably broad because the government "could collect *all* communications" between entire geographical areas, such as "New York and London" as long as the "nominal" or "ostensible" targets were foreign citizens outside the United States. (Defs. Mot. 25). 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 IV.D.1.a, there is no indication of any non-compliance by the government that would rebut that presumption.[38]

CLASSIFIED MATERIAL REDACTED

3. 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 would be 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 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*, 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").[39] The

[38] **CLASSIFIED MATERIAL REDACTED**

[39] **CLASSIFIED MATERIAL REDACTED**

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 and law enforcement 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.").[40]

Defendants contend (Defs. Mot. 40) that the minimization procedures are inadequate, despite their similarity to the procedures used in Title I FISA surveillance, because "minimization [under the FAA] is not individualized but programmatic; minimization procedures apply not to surveillance of specific targets but rather to surveillance programs, the specific targets of which may be known only to the executive branch." To the contrary, Congress has recognized that the application of uniform minimization procedures to collection directed against multiple targets actually *enhances* the protection of U.S. person information. H. Rep. No. 95-1283, Pt. 1, at 75 ("It is the intention of the committee that minimization procedures be as uniform as possible for similar surveillances. . . . The

[40] **CLASSIFIED MATERIAL REDACTED**

application of uniform procedures to identical surveillances will result in a more consistent implementation of the procedures, will result in an improved capability to assure compliance with the procedures, and ultimately means a higher level of protections for the rights of U.S. persons."); *see United States v. Abu-Jihaad*, 531 F. Supp. 2d 299, 303 n.4 (D. Conn. 2008), *aff'd* 630 F.3d 102 (2d Cir. 2010) (noting that "the Attorney General has adopted standard minimization procedures that apply to every [Title I] FISA application"); *In re All Matters Submitted to Foreign Intelligence Surveillance Ct.*, 218 F. Supp. 2d 611, 615 (FISC 2002) (referring to "Standard Minimization Procedures for a U.S. Person Agent of a Foreign Power that are filed with the Court, which we continue to approve"). The sufficiency of the minimization procedures therefore does not depend on the identity of the particular target, but rather on whether the procedures 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 information about United States persons consistent with the government's 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).

Defendants further contend (Defs. Mot. 39) that the minimization procedures "bear little resemblance" to the Title I FISA procedures and permit the government to conduct "unfettered" surveillance. However, the procedures employed here provide materially equivalent protection to the procedures employed for Title I and III FISA 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 searches, 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.

Defendants also argue (Defs. Mot. 40) that the minimization is inadequate because the FISC lacks authority to supervise the government's compliance with minimization procedures. However, the FAA's oversight provisions require regular reporting to the FISC concerning the government's implementation of minimization procedures. 50 U.S.C. § 1881a(1). In addition, Rule 13 of the FISC's Rules of Procedures requires the government to report, in writing, all instances of non-compliance.[41] 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.[42]

Defendants further contend (Defs. Mot. 18, 39) that the minimization procedures are inadequate because they permit the government to query information already collected pursuant to Section 702 using terms associated with U.S. persons.[43] Defendants are 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, merely running queries in a database does not infringe on any significant privacy interest or trigger any fresh constitutional analysis. *See 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

---

[41] FISC R. P. 13.

[42] **CLASSIFIED MATERIAL REDACTED**

[43] **CLASSIFIED MATERIAL REDACTED**

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 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).[44]

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

---

[44] A rule that every query, dissemination, or use of Section 702-obtained information amounts to a separate search under the Fourth Amendment would not only be contrary to these cases but also would be 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.

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"). 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.

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 FISC-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 powerful 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 III.A.3.a.[45] 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. 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 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.*[46]

[45] Such queries also help the government counteract operational security measures such as hiding operational communications in large amounts of non-operational communications in the hope of delaying the government's detection of those communications.

[46] **CLASSIFIED MATERIAL REDACTED**

In other words, electronic 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 an individual is an agent of a foreign power. 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.

4. 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

5. 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 (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).

6. 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.

d. Collection Under Section 702 Has Sufficient Particularity

Defendants' 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. (Defs. Mot. 33-42). In doing so, defendants characterize Section 702-authorized collection as "dragnet" surveillance that collects communications in "bulk." (*See, e.g., id.* at 11, 16, 32, 42). 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; and (2) the collection is designed to obtain foreign intelligence information within the scope of the certification approved by the court.[47]

CLASSIFIED MATERIAL REDACTED

Moreover, defendants' 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

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

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.

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 Youngstown*, 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 the defendants meets the Fourth Amendment's central requirement of reasonableness.

B. SECTION 702 IS CONSISTENT WITH ARTICLE III

Defendants contend (Defs. Mot. 44-48) 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. Defendants further maintain that review at this level of generality does not present a "case or controversy" within the meaning of Article III. 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).[48]

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

[48] 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).

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.").

Defendants are also incorrect in claiming that the lack of a particular factual context for the FISC's review of the government's certification renders the issue inappropriate for resolution by an Article III judge. Even the authority on which defendants rely recognizes that the standard is whether the questions presented to the FISC "are in a form such that a judge is capable of acting on them." *United States v. Megahey*, 553 F. Supp. 1180, 1197 (E.D.N.Y. 1982). 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. 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 tools through which the government implements Section 702. *See [Caption Redacted]*, 2011 WL 10945618, at *9 ("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. *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

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. 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 defendants' 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, *Ill. 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 12333 — 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.

Defendants 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 they 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.[49]

[49] 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

IV. THE SECTION 702 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, defendants also question the government's compliance with the applicable targeting and minimization procedures with respect to the specific information used in this case. (Defs. Mot. 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 certification(s), targeting procedures, and minimization procedures, all of which were reviewed and approved by the FISC, complied with the requirements for such certification(s) and procedures set forth in Section 702. Second, the Section 702 collection at issue in this case was conducted in accordance with those approved certification(s) and procedures.

A. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

---

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, defendants' 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. CLASSIFIED 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

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

V. DEFENDANTS' DISCOVERY MOTION SHOULD BE DENIED

Defendants request discovery on a number of theories: (1) that disclosure is required under the Due Process Clause (Defs. Mot. 48); (2) that adversarial proceedings are required either because of the uniqueness of the legal issues, a lack of precedent, on the defendants' supposition that they would craft better arguments if they knew more about the underlying classified information, on the basis of so-called misrepresentations to the FISC, or on the argument –previously rejected by this court in CIPA proceedings – that *ex parte* proceedings are disfavoured or inconsistent with due process (Defs. Mot. 49-60); and (3) the argument that a suppression motion cannot be crafted

without disclosure – an argument which is undercut by years of precedent to the contrary (Defs. Mot. 48). For the reasons set forth below, the defendants' 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 1881a collection, which is deemed to be Title I FISA 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]." *Id.* (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); *Abu-Jihaad*, 630 F.3d at 129; *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 THE FISA MATERIALS IS THE RULE

In light of these requirements, courts have consistently 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).[50] 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 lawfulness of 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). Thus, if this Court is able to determine the legality of the Section 1881a 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.

C. DEFENSE PARTICIPATION IS NOT NECESSARY TO 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 defendants' allegations to the contrary may be considered, and rejected, based on an examination of the classified record. Contrary to defendants' 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).

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

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

Defendants contend (Defs. Mot. 50-51) that the Court should grant disclosure because his motion presents "factually and legally complex" issues that the Court must resolve "without the aid of precedent."[51] That contention has no merit.

An order granting disclosure based simply on the fact that a FISA claim raises issues that have not previously been adjudicated would be inconsistent with the statutory scheme. After all, 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, in camera*, with disclosure the exception. Courts have been following that procedure for decades. *E.g., In re Grand Jury Proceedings*, 347 F.3d at 203; *El-Mezain*, 664 F.3d at 567; *Abu Jihaad*, 630 F.3d at 129; *Duggan*, 743 F.2d at 78. Moreover, the statute requires that courts review the FISA applications and orders *in camera* and *ex parte* before even contemplating disclosure. Thus, 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 his case raises novel issues.

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" "as a matter of statutory interpretation" because "[t]he language of section 1806(f) clearly anticipates that an *ex parte*, *in*

[51] In asserting the lack of any helpful precedent, Muhtorov again fails to mention the decision of the FISA Court of Review in *In re Directives*.

camera determination is to be the rule. Disclosure and an adversary hearing are the exception, occurring only when necessary." *Id.* (emphasis in original). Thus, Muhtorov's arguments conflict with *Belfield*, the clear statutory standard governing disclosure, and the process set forth in FISA for review of FISA suppression claims.

The defendants note (Defs. Mot. 52) that, "without disclosure," the Court and the defendants will "lose the benefit of informed arguments" from the defense. However, as noted above, whether disclosure might assist the defendants in effectively presenting their claims is not the relevant standard. FISA requires a finding by the Court, after an *ex parte, in camera* review, that disclosure "is necessary" for the Court to "make an accurate determination of the legality of the surveillance." 50 U.S.C. § 1806(f); *see* Kris & Wilson, National Security Investigations § 29:3 n.1 (2d ed. 2012) (describing legislative history of another FISA provision in which Congress emphasized that the term "necessary" meant "important and required," and not simply "useful or convenient").

Moreover, the defendants' contention runs 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." S. Rep. No. 701, 95th Cong., 2d Sess. 57 (1978); *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 it 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 S. Rep. No. 701, 95th Cong., 2d Sess. 63).[52]

Defendants contend (Defs. Mot. 52) that courts have suggested that factors such as "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," indicate that an adversary hearing may be warranted. They further contend that the government's "repeated misrepresentations to the FISC" establish the presence of those factors. (Defs. Mot. 52). However, the defendants fail 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, *in camera, ex parte* 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").[53]

---

[52] A prior version of the bill that became FISA would have allowed disclosure of the applications and orders "if there is a reasonable question as the legality of the surveillance and if disclosure would likely promote a more accurate determination of such legality or if such disclosure would not harm the national security." House Report at 10. That version, however, was not enacted by Congress. *See* H.R. Conf. Rep. No. 95-1720, 31-32, reprinted in 1978 U.S. Code Cong. & Admin. News 4048, 4060-61.

[53] The defendants' argument that they are entitled to a *Franks* hearing suffers from the same weakness. Defs. Mot. 56-57. A defendant cannot establish entitlement to a *Franks* hearing based on evidence of misrepresentations in some other case. If that were true, every defendant would be entitled to a *Franks* hearing simply by pointing to alleged misrepresentations in a different case.

Nor do the defendants' citations to statements in various FISC opinions, most of which do not involve Section 702, justify ordering disclosure of the Section 702 materials. Apart from the fact that those opinions have virtually no relevance to the present case, they underscore a more significant fact: the government takes its obligations under FISA and the Constitution seriously and candidly acknowledges and corrects deficiencies and compliance problems when it discovers them. *See* Comments of the Judiciary on Proposals Regarding the Foreign Intelligence Surveillance Act (Jan. 10, 2014) at 5, 7 (noting that the government generally exhibits a "high degree of candor" in *ex parte* proceedings before the FISC and that the government "routinely discloses in an application information that is detrimental to its case"), available at www.judiciary.senate.gov/resources/documents/113thCongressDocuments/upload/011413RecordSub-Grassley.pdf. To the extent that there are any issues concerning the lawfulness of the Section 1881a collection at issue, as raised in FISC opinions, those have been addressed in this pleading. Muhtorov's speculation therefore cannot overcome the statutory presumption favoring this Court's *ex parte* review.[54]

[54] None of the FISC opinions cited by the defendants have any bearing on the issues surrounding the use of information derived from the acquisition of foreign intelligence information conducted pursuant to Section 702 in this case. Only one FISC opinion cited by the defendants relates in any way to the acquisition of foreign intelligence information under Section 702. *See [Caption Redacted]*, 2011 WL 10945618. The defendants' reliance on that opinion, however, is misplaced. That opinion does not alter Section 1806's requirement that the district court first conduct an *in camera, ex parte* review of the government's submissions and only order disclosure if necessary to determine the legality of the Section 702 collection at issue. Moreover, the concerns expressed in that opinion applied only to one particular collection technique under Section 702, not to Section 702 collection as a whole, which the FISC approved as lawful. *See id.* at *14, 28. Thus, if that technique is not at issue in this case, then the FISC opinion supports the proposition that Section 702 collection is constitutional.

CLASSIFIED MATERIAL REDACTED

The defendants' contend that disclosure of the Section 702 materials is required under *Brady v. Maryland*, 373 U.S. 83 (1963), on the ground that the materials "likely" will contain "information favorable" to the motion to suppress. Defs. Mot. 57-59. The government understands and has every intention of complying with its discovery obligations. The defendants are not entitled to go on a "fishing expedition" of the government's files on the mere supposition that they may contain exculpatory information. That contention has no merit.

Where disclosure is not necessary to make an accurate determination of the legality of the surveillance, FISA prohibits disclosure "except to the extent that due process requires discovery or disclosure." 50 U.S.C. § 1806(g). The due process requirement embraced by FISA is coterminous with the *Brady* standard. *See United States v. Spanjol*, 720 F. Supp. 55, 59 (E.D. Pa. 1989). However, contrary to defendants' speculation, none of the Section 702 materials submitted herewith are "material" within the meaning of *Brady*. The defendants' argument that due process requires disclosure of FISA materials based on the defendants' allegation that the materials "likely" will assist them in litigating their suppression motion would, again, apply in every FISA case and is therefore inconsistent with the numerous cases upholding FISA's *ex parte* review procedure against constitutional challenges. *See, e.g., El-Mezain*, 664 F.3d at 567-69; *Damrah*, 412 F.3d at 624-25; *United States v. Isa*, 923 F.2d 1300, 1306-07 (8th Cir. 1991); *Ott*, 827 F.2d at 476-77; *Belfield*, 692 F.2d at 148. Likewise, even if, as the defendants contend (Defs. Mot. 59), FISA's due process disclosure requirement incorporates the "relevant and helpful" standard from the CIPA context, rather than the more stringent *Brady* standard, the Section 702 materials are not discoverable under either standard.

Finally, the defendants contend that adversary process is required in this context by the Constitution's due process, right to counsel, and confrontation clauses. Defs. Mot. 61-64. As noted

above, that contention is inconsistent with decades of practice in FISA litigation and numerous cases upholding FISA's *in camera, ex parte* procedures against constitutional challenges. Muhtorov's argument also founders on the large body of non-FISA law allowing courts to hold *ex parte*, *in camera* hearings when necessary to protect an informant's safety, the integrity of an ongoing investigation, or some other important interest. *See Isa*, 923 F.2d at 1307; *United States v. Falvey*, 540 F. Supp. 1306, 1315 (E.D.N.Y. 1982). Indeed, even before FISA came into existence, the Supreme Court authorized the adjudication of electronic surveillance *in camera, ex parte*. *See Taglianetti v. United States*, 394 U.S. 316, 317 (1969) (per curiam) ("Nothing [in the Supreme Court previous decisions] requires an adversary proceeding and full disclosure for resolution of every issue raised by an electronic surveillance"); *Giordano v. United States*, 394 U.S. 310, 314 (1969) ("Of course, a finding by the District Court that surveillance was lawful would make disclosure and further proceedings unnecessary."). More generally, the Supreme Court has "repeatedly declined to require the use of adversarial procedures to make probable cause determinations." *Kaley v. United States*, 134 S. Ct. 1090, 1103 (2014). In accordance with those principles, the government's undeniable interest in protecting ongoing national security investigations and intelligence sources and methods, coupled with the protections found in other parts of FISA, justifies limiting the defendants' right to review the FISA applications and orders. *See Isa*, 923 F.2d at 1307. Accordingly, defendants' request for discovery should be denied.

VI. DEFENDANTS ARE NOT ENTITLED TO A HEARING UNDER *FRANKS v. DELAWARE*

Defendants argue that they are entitled to a Franks hearing based on purported misrepresentations in the applications that led to the orders under which Muhtorov's communications were seized" and because of some perceived failure of the FISC to bar the

defendants' surveillance. Defs. Mot. 56, 62. For the reasons given below, the court should deny this request.

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, before the FISC 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); *Ning Wen*, 477 F.3d at 897. 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); *Duggan*, 743 F.2d at 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; *Mubayyid*, 521 F. Supp. 2d at 130-31.

The defendants' 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, 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.

Belfield, 692 F.2d at 148; *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.

(U) Defendants 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. 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 at 310; *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 defendants' attempt to hold a *Franks* hearing in this case without making the proper showing.

VII. CONCLUSION

Based on the above discussion and analysis, the government requests that the Court deny defendants' Motion to Suppress Evidence Obtained or Derived from Surveillance Under the FISA Amendments Act and Motion for Discovery.

Respectfully submitted this 9th day of May 2014.

JOHN WALSH
United States Attorney

/s/ Gregory Holloway
Assistant United States Attorney
District of Colorado

JOHN P. CARLIN
Assistant Attorney General
for National Security

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

/s/ Erin Creegan
Trial Attorney
Counterterrorism Section
National Security Division
United States Department of Justice