UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OHIO
WESTERN DIVISION

United States of America,

Plaintiff

Case No. 3:15-cr-358

v.

UNCLASSIFIED MEMORANDUM OPINION

Yahya Farooq Mohammad, et al.,

Defendants

Before me are several motions.[1] First, Defendants have requested the disclosure of Foreign Intelligence Surveillance Act ("FISA") material and the suppression of the evidence obtained or derived from electronic surveillance and physical searches conducted under FISA Titles I and III. (Doc. No. 148 at 1; Doc. No. 156 at 1.) These motions are denied.

Next, Defendants request the suppression of evidence obtained or derived from acquisitions made under FISA Section 702. (Doc. No. 146 at 1–2.) Defendants have also requested the disclosure of the FISA Section 702 materials relevant to this case. (Doc. No. 140 at 1.) These Section 702 motions are also denied.

And lastly, Defendants have requested an order directing the Government to provide notice and additional information about the surveillance it undertook in preparing this case. (Doc. No. 131 at 1.) This motion is denied as well.

[1] All but one of the motions were filed by Yahya Farooq Mohammad, who has since pleaded guilty. The other Defendants have, with limited exceptions, joined Farooq's motions and adopted his arguments. (*See* Doc. Nos. 142, 143, 145, 155, 156, 160.) Sultane Roome Salim brings the remaining motion, (Doc. No. 156 at 1), which Asif Ahmed Salim has joined, (Doc. No. 160 at 2).

I.

Defendants Yahya Farooq Mohammad, Ibrahim Zubair Mohammad, Sultane Roome Salim, and Asif Ahmed Salim were indicted on September 30, 2015, and charged with (Count 1) conspiracy to provide and conceal material support to terrorists, in violation of 18 U.S.C. § 2339A; (Count 2) providing material support to terrorists, in violation of 18 U.S.C. § 2339A; (Count 3) conspiracy to commit bank fraud, in violation of 18 U.S.C. § 1349 (brought against Farooq and Ibrahim only); and (Count 4) conspiracy to obstruct justice, in violation of 18 U.S.C. § 1512(k). (Doc. No. 1 at 12–72.)

The Government accuses Defendants of conspiring to provide, and actually providing, funds and other material support to Anwar al-Awlaki for the preparation and execution of terrorist attacks and killings. (*See* Doc. No. 1 at 12, 68.) The Government contends Defendants conspired to obstruct its investigation into their illicit fundraising by making false statements to the FBI and destroying or concealing records. (*Id.* at 65–67, 71–72.) And as to Farooq and Ibrahim, the Government additionally alleges that they conspired to raise money for al-Awlaki through various fraudulent credit card and PayPal transactions. (*Id.* at 68–71.)

Farooq has since pleaded guilty to the charges against him. (Doc. No. 284 at 1.) The other Defendants are scheduled to be tried on April 23, 2018. (Doc. No. 259 at 1.)

On December 21, 2015, the Government notified Defendants that it intends to offer into evidence, or otherwise use or disclose in any proceeding in this case, information obtained or derived from (i) electronic surveillance under FISA Title I (as to Sultane and Asif), (ii) physical searches under FISA Title III (as to Ibrahim, Sultane, and Asif), and (iii) acquisitions under FISA Section 702 (as to Ibrahim and Asif) under FISA. (*See* Doc. Nos. 28, 29, 30.)

In response to these notices, Defendants have filed several motions. In motions directed at FISA Titles I and III (Doc. Nos. 148, 156), Defendants have moved for (i) me to review the Government's applications for FISA surveillance and searches, (ii) the disclosure of the Government's applications for surveillance and searches, (iii) an evidentiary hearing pursuant to *Franks v. Delaware*, 438 U.S. 154 (1978), and (iv) the suppression of any evidence obtained or derived from illegally authorized or implemented surveillance or searches. (*See* Doc. No. 150 at 3; Doc. No. 156 at 1.)

In motions directed at FISA Section 702 (Doc. Nos. 140, 146), Defendants have requested (i) the disclosure of the Section 702 materials relevant to this case and (ii) the suppression of all evidence obtained or derived from acquisitions under Section 702. (Doc. No. 140 at 1; Doc. No. 146 at 1.)

And in a motion aimed broadly at all of the Government's surveillance and evidence-gathering methods (Doc. No. 131), Defendants request an order directing the Government to provide notice of "(1) each surveillance technique it used to obtain information about Defendant's communications or activities in its investigation; (2) the timing or duration of that surveillance; (3) the legal authority relied upon; and (4) the evidence obtained or derived from that surveillance." (Doc. No. 131 at 1.)

The Government opposes Defendants motions and has responded by filing classified and unclassified memoranda in opposition. The Government has also filed an affidavit signed by the Attorney General in which she declared under oath that "it would harm the national security of the United States to disclose or hold an adversary hearing with respect to the FISA Materials" in this matter. (Doc. No. 190 ¶ 3.) The filing of this affidavit triggers a statutory mandate directing me to "review in camera and ex parte the application, order, and such other materials relating to

the [FISA] 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 id.* § 1881e(a).

I have conducted the required in camera, ex parte review of the FISA materials and now address Defendants' motions. I first consider the motions for disclosure and suppression under FISA Titles I and III (Doc. Nos. 148, 156).

II.

Enacted in 1978, the Foreign Intelligence Surveillance Act, establishes a statutory framework under which executive branch agencies may collect foreign intelligence information. *See United States v. Aziz*, 228 F. Supp. 3d 363, 366 (M.D. Pa. 2017); *see* 50 U.S.C. § 1801, et seq. As part of this framework, Congress created two specialized courts: the Foreign Intelligence Surveillance Court ("FISC") and the Foreign Intelligence Surveillance Court of Review ("FISCR"). 50 U.S.C. § 1803. FISA authorizes the Chief Justice of the United States to designate eleven United States District Judges to sit as judges of the FISC. *Id.* § 1803(a)(1). FISC judges consider ex parte applications submitted by the executive branch for electronic surveillance and physical searches. *See id.* The FISCR, which is composed of three United States District or Circuit Judges designated by the Chief Justice, reviews denials by the FISC of applications for FISA intelligence collection. *Id.* § 1803(b).

FISA, as amended in 2001 under the USA PATRIOT Act ("Patriot Act") and as amended again in 2008 under the FISA Amendments Act ("FAA"), consists of eight titles. As relevant here, Title I (codified at 50 U.S.C. §§ 1801 to 1813) deals with electronic surveillance, Title III (codified at 50 U.S.C. §§ 1821–1829) deals with physical searches, and Section 702 (part of Title VII and codified at 50 U.S.C. § 1881a) deals with the acquisition of foreign intelligence

information from electronic communication service providers. Unlike surveillance under Titles I and III, Section 702 surveillance targets non-United States persons located abroad. *See* 50 U.S.C. § 1881a(b).

A. FISA Titles I and III

Titles I and III of FISA provide detailed procedures for the authorization and execution of electronic surveillance and physical searches.

1. Emergency Authorization and Standard FISA Application

The Government typically must apply for and obtain an order from the FISC before conducting electronic surveillance under Title I or engaging in physical searches under Title III. *See United States v. Huang*, 15 F. Supp. 3d 1131, 1136 (D.N.M. 2014). An exception to this general rule is when the Attorney General authorizes emergency surveillance or an emergency physical search. An emergency authorization is proper if the Attorney General

> (A) reasonably determines that an emergency situation exists with respect to the employment of electronic surveillance [or a physical search] to obtain foreign intelligence information before an order authorizing such surveillance [or physical search] can with due diligence be obtained;
>
> (B) reasonably determines that the factual basis for the issuance of an order . . . to approve such electronic surveillance [or physical search] exists;
>
> (C) informs, either personally or through a designee, a judge having jurisdiction . . . at the time of such authorization that the decision has been made to employ emergency electronic surveillance [or an emergency physical search]; and
>
> (D) makes an application . . . to a judge having jurisdiction . . . as soon as practicable, but not later than 7 days after the Attorney General authorizes such surveillance [or physical search].

50 U.S.C. § 1805(e)(1); *see id.* § 1824(e)(1).

In all other circumstances, the Government must apply for and obtain an order from the FISC before engaging in electronic surveillance under Title I or a physical search under Title III. The application to conduct electronic surveillance or a physical search must include

> (1) the identity of the [f]ederal officer making the application;
>
> (2) the identity, if known, or a description of the specific target of the electronic surveillance [or physical search, and, in the case of a physical search, a description of the information, material, or property to be seized, reproduced, or altered];
>
> (3) a statement of the facts and circumstances relied upon by the applicant to justify his belief that—
>
> > (A) the target of the electronic surveillance [or physical search] is a foreign power or an agent of a foreign power[, and, in the case of a physical search, the premises or property to be searched contains foreign intelligence information];
> >
> > (B) each of the facilities or places at which the electronic surveillance [or physical search] is directed is . . . or is about to be used, [owned, possessed by, or in transit to] a foreign power or an agent of a foreign power;
>
> (4) a statement of the proposed minimization procedures;
>
> (5) a description of the nature of the information sought and the type of communications or activities to be subjected to the [electronic] surveillance[, or, in the case of a physical search, a statement of the nature of the foreign intelligence sought and the manner in which the physical search is to be conducted];
>
> (6) A certification [of a high-ranking executive branch official]—
>
> > (A) that the certifying official deems the information sought to be foreign intelligence information;
> >
> > (B) that a significant purpose[2] of the surveillance [or physical search] is to obtain foreign intelligence information;

[2] As originally enacted, FISA required a high-ranking member of the executive branch to certify that "the purpose" of the surveillance was to obtain foreign intelligence information. *Aziz*, 228 F. Supp. 3d at 367. The required certification changed when Congress enacted the Patriot Act in 2001. *See id.* The Patriot Act amended FISA to require that a high-ranking executive branch official certify that the acquisition of

> (C) that such information cannot reasonably be obtained by normal investigative techniques;
>
> (D) that designates the type of foreign intelligence information being sought . . .; and
>
> (E) including a statement of the basis for the certification that—
>
> (i) the information sought is the type of foreign intelligence information designated; and
>
> (ii) such information cannot reasonably be obtained by normal investigative techniques;
>
> (7) a summary statement of the means by which the surveillance will be effected and a statement whether physical entry is required to effect the [electronic] surveillance[, and, in the case of a physical search of the residence of a United States person, the Attorney General shall state what investigative techniques have previously been utilized to obtain the foreign intelligence information concerned and the degree to which these techniques resulted in acquiring such information];
>
> (8) a statement of the facts concerning all previous applications that have been made to any judge under this subchapter involving any of the persons, facilities, or places specified in the application, and the actions taken on each previous application; and
>
> (9) a statement of the period of time for which the electronic surveillance is required to be maintained . . . .

50 U.S.C. § 1804(a); *see id.* § 1823(a) (footnote added). The Attorney General must approve applications for electronic surveillance or physical search before they are presented to the FISC. *See id.* §§ 1804(a), 1823(a).

As used in FISA, "foreign intelligence information" encompasses "information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against— (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; [or] (B) . . . international terrorism . . . by a foreign power

---

foreign intelligence information is "a significant purpose" of the requested surveillance. *See id.*; 50 U.S.C. §§ 1804(a)(6)(B), 1823(a)(6)(B).

or an agent of a foreign power . . . ." 50 U.S.C. § 1801(e)(1); *see id.* § 1821(1). The term also encompasses "information with respect to a foreign power . . . that relates to, and if concerning a United States person is necessary to—(A) the national defense or the security of the United States; or (B) the conduct of the foreign affairs of the United States." *Id.* § 1801(e)(2); *see id.* § 1821(1).

A "United States person" encompasses United States citizens and aliens lawfully admitted for permanent residence in the United States. 50 U.S.C. § 1801(i); *see id.* § 1821(1).

A "foreign power" includes any "group engaged in international terrorism or activities in preparation therefor." 50 U.S.C. § 1801(a)(4); *see id.* § 1821(1). And an "agent of a foreign power" encompasses "any person other than a United States person, who . . . acts in the United States . . . as a member of a foreign power . . . irrespective of whether the person is inside the United States" or "engages in international terrorism or activities in preparation therefore." *Id.* § 1801(b)(1); *see id.* § 1821(1). An agent of a foreign power also encompasses "any person who . . . knowingly engages in . . . international terrorism, or activities that are in preparation therefore, for or on behalf of a foreign power" or "knowingly aids or abets any person in the conduct of [the activities just described] or knowingly conspires with any person to engages in [those] activities." *Id.* § 1801(b)(2); *see id.* § 1821(1).

Also referenced in the application requirements above (and in other FISA titles), "minimization procedures" are specific procedures, adopted by the Attorney General, that are, among other things,

> reasonably designed in light of the purpose and technique of the particular surveillance [or physical search], to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States person consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information.

50 U.S.C. § 1801(h)(1); *see id.* § 1821(4)(A). Notably, minimization procedures 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." *Id.* §§ 1801(h)(3), 1821(4)(C).

2. FISC Order

After reviewing the Government's application, the FISC will issue an ex parte order authorizing electronic surveillance or physical searches if it finds that

> (1) the application has been made by a [f]ederal officer and approved by the Attorney General;
>
> (2) on the basis of the facts submitted by the applicant there is probable cause to believe that—
>
> > (A) the target of the electronic surveillance [or physical search] is a foreign power or an agent of a foreign power: *Provided*, That no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States; and
> >
> > (B) each of the facilities or places at which the electronic surveillance [or physical search] is directed is . . . or is about to be used, [owned, possessed by, or is in transit to] a foreign power or an agent of a foreign power;
>
> (3) the proposed minimization procedures meet the definition of minimization procedures under [FISA]; and
>
> (4) the application . . . contains all statements and certifications required [under § 1804 (with respect to electronic surveillance) or § 1823 (with respect to a physical search)] . . . and, if the target is a United States person, the certification or certifications are not clearly erroneous . . . .

50 U.S.C. § 1805(a); *see id.* § 1824(a).

A FISC order must specify

> (A) the identity, if known, or a description of the specific target of the electronic surveillance [or physical search] . . . ;

(B) the nature and location of each of the facilities or places at which the electronic surveillance will be directed, if known[, or, in the case of a physical search, the nature and location of each of the premises or property to be searched];

(C) the type of information sought to be acquired and the type of communications or activities to be subjected to the surveillance[, or, in the case of a physical search, the type of information, material, or property to be seized, altered, or reproduced];

(D) the means by which the electronic surveillance will be effected and whether physical entry will be used to effect the surveillance[, or in the case of a physical search, a statement of the manner in which the search is to be conducted and, whenever more than one physical search is authorized under the order, the authorized scope of each search and a description of the minimization procedures applicable to the information acquired by each search]; and

(E) the period of time during which the electronic surveillance [or physical searches are] approved.

50 U.S.C. § 1805(c)(1); *see id.* § 1824(c)(1). A FISC order must also direct that the Government follow the applicable minimization procedures. *Id.* §§ 1805(c)(2)(A), 1824(c)(2)(A).

Electronic surveillance and physical searches targeting a United States person may be approved for up to 90 days; surveillance and searches targeting a non-United States person may be approved for up to 120 days. *See* 50 U.S.C. §§ 1805(d)(1), 1824(d)(1). An extension to this time frame may be obtained, but only if the United States submits another application that complies with FISA's requirements. *See id.* §§ 1805(d)(2), 1824(d)(2). Extensions relating to a United States person may be approved for up to 90 days; those relating to a non-United States person may be approved for up to one year. *See id.*

3. District Court Review

An "aggrieved person" can move to suppress FISA-obtained or -derived evidence that the Government seeks to use against him in a trial, hearing, or other proceeding in or before any court. *See* 50 U.S.C. §§ 1806(e), 1825(f)(1). A person is aggrieved under FISA if he is the target

of, or was subject to, electronic surveillance, *see id.* § 1801(k), or if his premises, property, information, or material is the target of, or was subject to, a physical search, *see id.* § 1821(2). An aggrieved person can move for suppression on the grounds that (1) the information was unlawfully acquired or (2) the surveillance or physical search was not made in conformity with the FISC's order. *See id.* §§ 1806(e), 1825(f)(1).

When considering a motion to suppress evidence obtained through FISA collection, a court must review the Government's applications, the FISC's orders, and any documentation describing the execution of the collection. *See United States v. Alwan*, No. 1:11-CR-13, 2012 WL 399154, at *7–8 (W.D. Ky. Feb. 7, 2012).

a. Reviewing FISA Applications

A district court's primary task in reviewing an application for FISA collection is to ensure that it contains all the statutorily mandated elements. *See Alwan*, 2012 WL 399154, at *7. When an application "was properly made and earlier approved by a FISA judge, it carries a strong presumption of veracity and regularity in a reviewing court." *Id.* (quoting *United States v. Pelton*, 835 F.2d 1067, 1076 (4th Cir. 1987)). Consequently, district courts subject the Government's FISA applications to minimal scrutiny on review. *Id.*

Like the application itself, the certification appended to a FISA application is also presumed valid and subjected only to minimal scrutiny. *See, e.g., United States v. Badia*, 827 F.2d 1458, 1463 (11th Cir. 1987); *United States v. Duggan*, 743 F.2d 59, 77 & n.6 (2d Cir. 1984). Neither the FISC nor a reviewing district court should "second-guess the executive branch official's certification." *Duggan*, 743 F.2d at 77. The reviewing court's role is merely to ensure the certifications were properly made. *See id.*; *United States v. Ahmed*, No. 1:06-cr-147, 2009 U.S. Dist. LEXIS 120007, at *20 (N.D. Ga. Mar. 19, 2009).

b. Reviewing FISC Orders

A district court must review FISC orders to ensure they contain the statutorily required findings, specifications, and directions. *See Alwan*, 2012 WL 399154, at *8, *10.

One of the most critical findings the FISC must make before authorizing electronic surveillance is that probable cause exists to believe (a) the target of the surveillance or search is a foreign power or an agent of a foreign power and (b) each of the facilities or places at which the surveillance or search is targeted is or is about to be owned, used, possessed by, or is in transit to or from a foreign power or an agent of a foreign power. *See* 50 U.S.C. §§ 1805(a)(2), 1824(a)(2). There is some disagreement on the standard district courts should apply when reviewing the adequacy of the FISC's probable cause determination. A minority of courts has held that a standard deferential to the FISC's determination is appropriate. *See Aziz*, 228 F. Supp. 3d at 374. This Court, however, agrees with "[t]he more robust line of authority," which has concluded that a de novo standard applies. *Id.*; *see, e.g.*, *United States v. Hassan*, 742 F.3d 104, 138–39 (4th Cir. 2014) (stating that the district court reviewed the probable cause determinations de novo in accordance with the Fourth Circuit's precedent); *United States v. Elshinawy*, No. 16-0009, 2017 WL 1048210, at *9 (D. Md. Mar. 20, 2017) (applying a de novo standard of review); *United States v. Mubayyid*, 521 F. Supp. 2d 125, 131 (D. Mass. 2007) (same); *United States v. Rosen*, 447 F. Supp. 2d 538, 545 (E.D. Va. 2006) (same).

Consequently, in conducting my review of the Title I and Title III materials, I accord a presumption of validity to the Government's applications and supporting certifications, and I review de novo the FISC's probable cause determinations. *See Duggan*, 743 F.2d at 77 & n.6; *Alwan*, 2012 WL 399154, at *7–8; *Mubayyid*, 521 F. Supp. 2d at 131; *Rosen*, 447 F. Supp. 2d at 545.

c. Ex Parte and In Camera Procedure

The Government has filed an affidavit from the Attorney General in which she stated under oath that disclosure or an adversary hearing would harm the national security of the United States. (Doc. No. 190 ¶ 3.) When the Government files such an affidavit, the district court must review the FISA materials in camera and ex parte. 50 U.S.C. § 1806(f). And when the Government files such an affidavit, the court may only order the disclosure of the FISA materials "where such disclosure is necessary to make an accurate determination of the legality of the surveillance." *Id.* § 1806(f). Disclosure may be necessary under FISA

> where the court's initial review of the application, order, and fruits of the surveillance indicates that the question of legality may be complicated by factors 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, calling into question compliance with the minimization standards contained in the order."

United States v. Belfield, 692 F.2d 141, 147 (D.C. Cir. 1982) (quoting S. Rep. No. 95-701, at 64 (1978)). If, in other words, the court concludes that it can determine, without assistance or input from the aggrieved party, whether the FISA surveillance was lawful, the court may not order disclosure of the FISA materials. *See* 50 U.S.C. § 1806(f); *United States v. Amawi*, 531 F. Supp. 2d 832, 837 (N.D. Ohio 2008).

If the court determines based on its in camera and ex parte review that the FISA collection was lawfully authorized and conducted in conformity with the FISC's orders, the court must deny the aggrieved party's motions for suppression and disclosure "except to the extent that due process requires discovery or disclosure." 50 U.S.C. § 1806(g). Courts have interpreted this to mean that disclosure is limited to that required under *Brady v. Maryland*, 373 U.S. 83 (1963). *See Aziz*, 228 F. Supp. 3d at 370; *Amawi*, 531 F. Supp. 2d at 837.

B. Disclosure of the FISA Title I and Title III Materials

I have reviewed, in camera and ex parte, the Title I and Title III materials submitted by the Government. And through this review, I conclude that I can determine, on my own, whether the challenged FISA collection was lawful. I have not observed in the materials any complicating factors, such as misrepresentations of fact, vague identifications of surveillance targets, or evidence of significant non-foreign intelligence collection. *See Belfield*, 692 F.2d at 147. Disclosure is, accordingly, not necessary to make an accurate determination of the legality of the surveillance, *see* 50 U.S.C. §§ 1806(f), and Defendants' request for the disclosure of the FISA materials is denied.

Defendants stress that disclosure of FISA material is permitted to the extent that due process requires it. (Doc. No. 150 at 25–26 (citing 50 U.S.C. § 1806(g)).) The due process exception does not apply here though. Courts have interpreted the exception narrowly; it encompasses only those materials that would be discoverable under *Brady*. *See Aziz*, 228 F. Supp. 3d at 370; *Amawi*, 531 F. Supp. 2d at 837. And here, my review of the FISA materials reveals no exculpatory information that would need to be disclosed under *Brady*.

As an additional argument for disclosure, Defendants contend that ex parte proceedings, like those mandated under FISA, are "antithetical to the adversary system that is the hallmark of American criminal justice" and that due process, therefore, requires defense counsel's participation in reviewing the FISA materials. (Doc. No. 150 at 26.)

Defendants have legitimate concerns regarding the fairness of ex parte proceedings. These types of proceedings, however, are not foreign to the American criminal justice system. *See United States v. Daoud*, 755 F.3d 479, 482 (7th Cir. 2014) ("The judge appears to have believed that adversary procedure is always essential to resolve contested issues of fact. That is

an incomplete description of the American judicial system in general and the federal judicial system in particular. There are *ex parte* or *in camera* hearings in the federal courts as well as hearings that are neither or both."); *United States v. Isa*, 923 F.2d 1300, 1307 (8th Cir. 1991) ("Courts often conduct *in camera* reviews in criminal proceedings when, as here, the defendant's right of confrontation is subordinated to competing interests of society.").

Nor are ex parte proceedings inherently unconstitutional or otherwise unlawful, as Defendants seem to suggest. *See Daoud*, 755 F.3d at 482–83. Indeed, numerous courts have found FISA's ex parte proceedings permissible. *See, e.g.*, *Isa*, 923 F.2d at 1306–07 (concluding that the Sixth Amendment right of confrontation is not violated by FISA's ex parte, in camera review procedures); *United States v. Belfield*, 692 F.2d 141, 147, 149 (D.C. Cir. 1982) ("The language of section 1806(f) clearly anticipates that an *ex parte*, *in camera* determination is to be the rule. Disclosure and an adversary hearing are the exception, occurring *only* when necessary. . . . [Moreover,] [a] claim that disclosure and an adversary hearing are constitutionally required goes directly contrary to all pre-FISA precedent on point. In this circuit and in others, it has constantly been held that the legality of electronic, foreign intelligence surveillance may, even should, be determined on an *in camera*, *ex parte* basis."); *United States v. Thomas*, 201 F. Supp. 3d 643, 650 (E.D. Pa. 2016) ("[T]he Court can safely reject Defendant's apparent contention that FISA's *ex parte* provisions are *per se* unlawful."); *United States v. Nicholson*, No. 09-CR-40, 2010 WL 1641167, at *3 (D. Or. Apr. 21, 2010) ("FISA's *in-camera* review provisions have been held to be constitutional."). And as most pertinent here, the Sixth Circuit has already rejected an argument similar to Defendants', holding that "FISA's requirement that the district court conduct an ex parte, in camera review of FISA materials does not deprive a defendant of due process." *United States v. Damrah*, 412 F.3d 618, 624 (6th Cir. 2005) ("There is likewise no

merit to Damrah's argument that *Alderman v. United States*, [394 U.S. 165 (1969)], mandates that surveillance materials [be produced] and an adversarial hearing be conducted before a district court can determine whether the surveillance was authorized and lawfully conducted. In *Alderman*, the issue was whether surveillance materials should be produced and an adversarial hearing conducted where the prosecution planned to use evidence from surveillance that had already been deemed unlawful."). Adhering to the Sixth Circuit's conclusion that FISA's ex parte and in camera procedures do not run afoul of constitutional due process requirements, I find that Defendants' argument lacks merit.

C. Suppression of FISA-Obtained or -Derived Evidence

Defendants next move for suppression of evidence obtained or derived from surveillance and physical searches conducted under FISA Titles I and III. They advance two arguments—one constitutional and one statutory. Defendants contend that Titles I and III violate the Fourth Amendment. (Doc. No. 150 at 31–35.) And Defendants highlight several issues that might cause the surveillance and searches to run afoul of FISA's statutory requirements. (*Id.* at 2–3.)

1. Fourth Amendment Argument

Defendants' constitutional argument focuses on FISA's amendment by the Patriot Act in 2001. (*See* Doc. No. 150 at 31–32.) As amended, FISA allows for surveillance when "a significant purpose" of the collection is the acquisition of foreign intelligence information. (*Id.* at 32 (quoting 50 U.S.C. §§ 1804(a)(6)(B), 1823(a)(6)(B)) (internal quotation marks omitted).) Prior to the amendment, FISA permitted surveillance only when "the purpose" of the surveillance was to obtain foreign intelligence information. *Aziz*, 228 F. Supp. 3d at 367. This change, Defendants argue, allows the Government to bypass the Fourth Amendment when

gathering evidence for a criminal prosecution if the Government simply certifies that a significant purpose of the FISA collection is the acquisition of foreign intelligence information.

Defendants acknowledge that courts have consistently upheld the constitutionality of the "significant purpose" standard. (Doc. No. 150 at 33.) They suggest, however, that these decisions should be revisited because they were issued before "the widely publicized public disclosures regarding the expansive nature of [FISA] Section 702's PRISM and [u]pstream collections—particularly insofar as they involve the collection of domestic communications of American citizens." (*Id.*) Because these surveillance programs allegedly "vacuum-up an untold number of domestic communications," courts should no longer "naively accept[] that the purpose of FISA surveillance is foreign intelligence." (*Id.* at 33–34.)

Controlling precedent decides this issue. In 2005, the Sixth Circuit rejected a Fourth Amendment challenge to FISA's procedures. *Damrah*, 412 F.3d at 625. The court explained in *Damrah* that the defendant's Fourth Amendment challenge lacked merit, as "FISA has uniformly been held to be consistent with the Fourth Amendment." *Id.*; *see also Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 421 n.8 (2013) (In *Damrah*, "the Sixth Circuit ultimately held that FISA's procedures are consistent with the Fourth Amendment."). *Damrah* has not been overturned or altered in light of the public disclosures regarding PRISM and upstream collections. And consequently, *Damrah* forecloses Defendants' constitutional challenge.[3]

2. Statutory Argument

Defendants' second suppression argument challenges the Government's adherence to FISA's statutory requirements. (*See* Doc. No. 150 at 2–3.) Defendants request suppression based

[3] Although Defendants suggest in passing that FISA, as amended by the Patriot Act, may violate other constitutional provisions (i.e., the First, Fifth, and Sixth Amendments), Defendants' constitutional argument focuses exclusively on the Fourth Amendment implications of FISA's "significant purpose" language. (*See* Doc. No. 150 at 31–35.)

on various potential statutory violations: (1) the FISA applications may have failed to establish probable cause that Defendants, or whomever was targeted, was a "foreign power" or "an agent of a foreign power"; (2) the FISA applications may contain intentional or reckless material falsehoods or omissions; (3) the primary purpose of the electronic surveillance or physical searches may have been to obtain evidence of domestic criminal activity and not foreign intelligence information or, in other words, capturing foreign intelligence information may not have been a "significant purpose" of the surveillance or searches; (4) the surveillance or searches may have been impermissibly based on activity protected by the First Amendment; (5) the Government may have been able to obtain the evidence collected through the surveillance or searches through normal investigative techniques; (6) the Government may not have made the required certifications in the FISA applications, may have failed to obtain any necessary extension of prior FISA orders, or may have continued the surveillance or searches after any basis for such initial surveillance was no longer valid; (7) the Government may not have established or abided by the appropriate minimization procedures; (8) the surveillance or searches may have been based impermissibly on acquisitions conducted pursuant to FISA Section 702; and (9) the Government may have violated other provisions of FISA or the First or Fourth Amendments, in manners unknown to Defendants. (*Id.*; Doc. No. 156 at 9–17.)

Based on my in camera, ex parte review of the Title I and Title III materials, I find Defendants' concerns unwarranted. The FISA applications contained the statutorily required elements. The FISC's orders contained the necessary elements and properly found the existence of probable cause. And the surveillance and searches were conducted in compliance with the FISC's orders. Defendants are, consequently, not entitled to suppression of evidence obtained or derived from surveillance and physical searches conducted under FISA Titles I and III.

D. *Franks* Hearing

For their last argument relating to Titles I and III, Defendants move for an evidentiary hearing under *Franks v. Delaware*, 438 U.S. 154, 155–56 (1978); Defendants request a *Franks* hearing so they can explore the veracity of the information set forth in the Government's applications. (Doc. No. 150 at 18–21.)

Under *Franks*, a criminal defendant may challenge the truthfulness of factual statements in an affidavit of probable cause through an evidentiary hearing. *See Franks*, 438 U.S. at 155–56, 171–72. When a defendant makes "a substantial preliminary showing" that the affidavit in question contains a false statement which was (1) knowingly or recklessly made and (2) necessary to the finding of probable cause, the court must conduct an evidentiary hearing to examine the sufficiency of the affidavit. *Id.* at 155.

The Sixth Circuit has not explicitly held that *Franks* applies to FISA applications and orders. *See Damrah*, 412 F.3d at 624–25. The Sixth Circuit has indicated, however, that if *Franks* does apply in the FISA context, the threshold burden under *Franks* (i.e., making a substantial preliminary showing that the affidavit contains a false statement) should also apply. *See id.*

I recognize the challenge faced by a defendant in making a substantial preliminary showing that a FISA application contains a false statement when the defendant does not have access to the application. But the threshold burden exists nonetheless. *See Mubayyid*, 521 F. Supp. 2d at 131 ("The balance struck under FISA—which is intended to permit the gathering of foreign intelligence under conditions of strict secrecy, while providing for judicial review and other appropriate safeguards—would be substantially undermined if criminal defendants were

granted a right of disclosure simply to ensure against the possibility of a *Franks* violation."). And here, Defendants have failed to satisfy that burden.

Defendants support their request for a *Franks* hearing with a discussion of a 2002 FISC decision, *In re All Matters Submitted to the Foreign Intelligence Surveillance Court*, 218 F. Supp. 2d 611, 620–21 (FISC 2002), in which the FISC reported that "[i]n September 2000, the government came forward to confess error in some 75 FISA applications related to major terrorist attacks directed against the United States"; these errors "related to misstatements and omissions of material facts." *Id.* at 620. Defendants argue that these issues were not isolated or resolved—as revealed by a March 2006 Department of Justice Inspector General report, which found that the FBI had frequently violated its own wiretapping and other intelligence-gathering procedures in the two years preceding the report. (Doc. No. 150 at 20–21 (citing U.S. Dep't of Justice, Office of the Inspector Gen., *A Review of the FBI's Handling of Intelligence Related to the September 11 Attacks (November 2004)* 24–25, 29 (2006)).)

Defendants' argument falls flat. The Government's errors from more than a decade ago do not amount to a substantial preliminary showing that an application for FISA collection relevant to this case contains a false statement which was knowingly or recklessly made and necessary to the finding of probable cause. I also note that in my review of the FISA applications relevant to this case, I have not observed any false statements, let alone false statements made knowingly or recklessly that would be necessary to the finding of probable cause. Defendants' request for a *Franks* hearing is denied.

I next consider the motions for disclosure and suppression under FISA Section 702 (Doc. Nos. 140, 146).

III.

A. FISA Section 702

As originally enacted, FISA defined "electronic surveillance" to cover four types of domestically-focused foreign intelligence collection activities. *See* 50 U.S.C. § 1801(f); *United States v. Hasbajrami*, No. 11-CR-623, 2016 WL 1029500, at *4 (E.D.N.Y. Mar. 8, 2016). Because the definition did not apply to surveillance conducted outside the United States, Congress decided to modernize FISA by enacting, in 2007, the Protect America Act ("PAA"). *Hasbajrami*, 2016 WL 1029500, at *4. Under the PAA, the Director of National Intelligence ("DNI") and the Attorney General could authorize the acquisition of foreign intelligence information concerning persons reasonably believed to be outside the United States. *Id.* To authorize an acquisition, the DNI and the Attorney General had to certify (i) that there were reasonable targeting procedures in place to ensure that the surveillance targeted persons reasonably believed to be outside the United States, (ii) that the minimization procedures in place satisfied FISA's requirements, and (iii) and that a significant purpose of the acquisition was to obtain foreign intelligence information. *Id.* The PAA, however, expired in February 2008 due to a sunset provision. *Id.* at *5. In response, Congress enacted the FISA Amendments Act in July 2008. *Id.*

Section 702 of the FAA, codified at 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 targeting the communications of non-U.S. persons located abroad." *Clapper*, 568 U.S. at 404. Section 702, unlike FISA Titles I and III, allows for foreign intelligence acquisition without a requirement that the Government first demonstrate probable cause that the target of the collection is a foreign power or agent of a foreign power. *Id.* Also unlike the surveillance and searches conducted under Titles I and III, under Section 702, the

Government can engage in foreign intelligence collection without first specifying the nature and location of each of the facilities or places at which the acquisition will occur. *Id.*

Congress reauthorized Section 702 acquisitions in January 2018 with the passage of the FISA Amendments Reauthorization Act of 2017.

1. Authorization

The Attorney General and the DNI may, upon the issuance of an order from the FISC, 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).[4] An authorization for Section 702 acquisition is subject to several limitations. The authorization

> (1) may not intentionally target any person known at the time of acquisition to be located in the United States;
>
> (2) may not intentionally target a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States;
>
> (3) may not intentionally target a United States person reasonably believed to be located outside the United States;
>
> (4) 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; [and]
>
> (5) may not intentionally acquire communications that contain a reference to, but are not to or from, a target of an acquisition authorized under subsection (a), except as provided under section 103(b) of the FISA Amendments Reauthorization Act of 2017; and
>
> (6) shall be conducted in a manner consistent with the [Fourth Amendment].

Id. § 1881a(b).

2. Submission to the FISC

[4] "Foreign intelligence information" has the same definition in § 1881a that it has in § 1801(e). *See* 50 U.S.C. § 1881(a).

Before the Government can acquire foreign intelligence information under Section 702, the Government must, with limited exceptions, obtain the FISC's approval of (1) the Government's certification regarding the proposed collection, (2) the applicable targeting procedures, and (3) the applicable minimization procedures. *See* 50 U.S.C. § 1881a(a), (c)(1)(B), (h)(1)(A), (j).

In the Government's certification, the Attorney General and the DNI must attest that

(1) There are targeting procedures in place, which have been or will be submitted for approval by the FISC, that are reasonably designed to ensure that the acquisition is limited to targeting person 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 FISA Titles I and III (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 limitations set forth in § 1881a(b) and to ensure that an application for a FISC order is filed;

(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 set forth in § 1881a(b). 50 U.S.C. § 1881a(h)(2)(A).

The Government's certification must include copies of the targeting and minimization procedures. *Id.* § 1881a(h)(2)(B). The certification must "be supported, as appropriate, by the affidavit of any appropriate official in the area of national security" who is either "appointed by the President, by and with the advice and consent of the Senate" or "the head of an element of the intelligence community." *Id.* § 1881a(h)(2)(C). And the certification must include either "an effective date for the authorization that is at least 30 days after the submission of the written certification to the [FISC]" or, if the acquisition has already begun or the effective date is less than 30 days after the certification's submission, "the date the acquisition began or the effective date for the acquisition." *Id.* § 1881a(h)(2)(D).

The Government's targeting procedures must be reasonably designed to (a) ensure that any authorized acquisition "is limited to targeting persons reasonably believed to be located outside the United States" and (b) "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). And the Government's minimization procedures must comport with the definition of the term as found in FISA Titles I and III (50 U.S.C. §§ 1801(h), 1821(4)). *Id.* § 1881a(e)(1).

3. FISC Order

The FISC must review (1) the Government's certification, (2) the applicable targeting procedures, and (3) the applicable minimization procedures, along with any amendments to the certification and procedures. 50 U.S.C. § 1881a(j)(1)(A).[5] The FISC reviews the certification to ensure that it contains all the required elements. *Id.* § 1881a(j)(2)(A). And the FISC reviews the targeting and minimization procedures to assess whether they comport with the requirements

[5] Under the FISA Amendments Reauthorization Act of 2017, the FISC must also review the querying procedures adopted by the Attorney General and the DNI. *See* 50 U.S.C. § 1881a(f)(1), (j)(1)(A). This newly added requirement is not implicated in the present case.

described above. *Id.* § 1881a(j)(2)(B), (C). The FISC must conduct this review not later than 30 days after receiving the Government's submission. *Id.* § 1881a(j)(1)(B).

In contrast to FISC approval of surveillance and searches conducted under FISA Titles I and III, FISC approval of Section 702 acquisitions does not entail an individualized court order for each person to be targeted. *Hasbajrami*, 2016 WL 1029500, at *5. Rather, the FISC approves annual submissions by the Attorney General and the DNI, thereby authorizing the acquisition of foreign intelligence information through the targeting of non-U.S. persons reasonably believed to be located outside the United States. *See* 50 U.S.C. § 1881a(a), (i)(3); *Hasbajrami*, 2016 WL 1029500, at *5.

If the FISC finds that the Government's certification contains the required elements and that the targeting procedures and minimization procedures comply with the statutory requirements and with the Fourth Amendment, the FISC "shall enter an order approving the certification and the use, or continued use [in limited circumstances], of the procedures for the acquisition." 50 U.S.C. § 1881a(j)(3)(A). If, however, the FISC finds deficiencies in the certification, targeting procedures, or minimization procedures, the FISC must issue an order directing the Government to—at the Government's election and to the extent required by the order—(i) correct, within 30 days, any deficiency identified by the order or (ii) cease, or not begin, the implementation of the authorization. *Id.* § 1881a(j)(3)(B).

4. Section 702 Acquisition

There are two types of Section 702 collection: PRISM and upstream. *Hasbajrami*, 2016 WL 1029500, at *6. When utilizing PRISM collection, the Government identifies the user accounts it wants to monitor and sends a "selector"—a specific communications facility, such as a target's email address or telephone number—to the relevant communications service provider.

Id. The Government then compels the service provider, through a directive, to provide it with communications sent to or from the selector. *Id.* This process is known as "tasking" the selector. *See id.* PRISM collection, which intercepts "to/from" communications, can result in the interception of communications with U.S. persons if the target communicates with such a person. *Id.*

The Government has represented this case does not involve upstream collection. (Doc. No. 191 at 19.) For background though, upstream collection involves the acquisition of communications through the compelled assistance of the providers that control the telecommunications backbone within the United States. *Hasbajrami*, 2016 WL 1029500, at *6. As with PRISM collection, upstream collection intercepts "to/from" communications. *Id.* Upstream, however, also allows for the interception of "about" communications, which are communications that refer to, or are "about," a particular selector. *Id.* If a targeted email address were to appear in the body of an email, that email would, for example, constitute an "about" communication. *Id.* Due to its interception of "about" communications, upstream collection can result in the acquisition of wholly domestic communications of non-targeted persons. *See id.*

5. Oversight

Section 702 requires that, at least every six months, the Attorney General and the DNI periodically assess the Government's compliance with the targeting procedures, minimization procedures, and relevant compliance guidelines. 50 U.S.C. § 1881a(m)(1). The Attorney General and the DNI must submit those assessments to the FISC and to congressional oversight committees. *Id.*

The Inspector General of the Department of Justice and the Inspector General of each element of the intelligence community authorized to acquire information through Section 702

must, among other things, review the number of Section 702 targets that were later determined to be located in the United States. 50 U.S.C. § 1881a(m)(2). The head of each element of the intelligence community conducting Section 702 acquisitions must, annually, conduct a similar review. *Id.* § 1881a(m)(3).

Additionally, the Attorney General must, at least every six months, "fully inform" the relevant congressional oversight committees about the implementation of Section 702. 50 U.S.C. § 1881f(a).

6. District Court Review

Information acquired through Section 702 surveillance is "deemed to be information acquired from an electronic surveillance pursuant to [FISA Title I]" for purposes of an aggrieved person's motion to suppress. 50 U.S.C. § 1881e(a)(1). So, under Section 702, an aggrieved person can move to suppress FISA-obtained or -derived evidence that the Government seeks to use against him in a trial, hearing, or other proceeding in or before any court. *See id.* § 1806(e). An aggrieved person can move for suppression on the grounds that (1) the information was unlawfully acquired or (2) the surveillance was not made in conformity with the FISC's order. *See id.*

And when the Government files an affidavit from the Attorney General—as the Government has done here—in which the Attorney General states under oath that disclosure or an adversary hearing would harm the national security of the United States, the district court must review the FISA materials in camera and ex parte. 50 U.S.C. § 1806(f). When an affidavit from the Attorney General has been filed, the court may only order the disclosure of the FISA materials "where such disclosure is necessary to make an accurate determination of the legality of the surveillance." *Id.*

B. Disclosure of Section 702 Materials

Defendants have moved for the disclosure of documents and materials concerning the Government's acquisitions under Section 702. (Doc. No. 140 at 1.) In support of this request, Defendants note that on August 11, 2016, the Office of the Director of National Intelligence released the 2015 Section 702 minimization procedures for the NSA, CIA, FBI, and National Counterterrorism Center ("NCTC"). (*Id.* at 2.) Defendants then point to a November 6, 2015 FISC opinion in which that court identifies numerous incidents where the intelligence agencies failed to comply with the approved minimization procedures. (*Id.* at 2–3.) Further, Defendants state that prosecutors in other national security cases have disclosed information about the PRISM and upstream collection programs. (*Id.* at 3.)

Defendants' arguments demonstrate that the Government has, on several occasions, voluntarily released to the public declassified information on FISA Section 702 surveillance. Here, however, aside from its representation that this case does not involve upstream collection, the Government has not offered to voluntarily release information. (*See* Doc. No. 191 at 19, 95.) Nor has the Government indicated the information sought by Defendants is, or will be, declassified. (*See id.* at 95.) Instead, the Government has submitted an affidavit in which the Attorney General stated under oath that disclosure or an adversary hearing on this matter would harm the national security of the United States. (*See id.* at 28.) Consequently, I may only order the disclosure of the FISA materials if the disclosure is necessary to make an accurate determination of the legality of the acquisition. 50 U.S.C. §§ 1806(f), 1881e(a).

I have reviewed, ex parte and in camera, the FISA Section 702 materials submitted by the Government. And through this review, I conclude that I can determine, on its own, whether the challenged Section 702 acquisition was lawful. Consequently, disclosure is not necessary to

make an accurate determination of the legality of the acquisition, *see* 50 U.S.C. §§ 1806(f), 1881e(a), and Defendants' request for the disclosure of the Section 702 materials is denied.

Disclosure of Section 702 material is also permitted "to the extent that due process requires" it. 50 U.S.C. § 1806(g); *see id.* § 1881e(a). The due process exception, however, does not apply here. As noted earlier, the exception encompasses only those materials that would be discoverable under *Brady*. *See Aziz*, 228 F. Supp. 3d at 370; *Amawi*, 531 F. Supp. 2d at 837. And here, my review of the Section 702 materials reveals no exculpatory information that would need to be disclosed under *Brady*.

C. Suppression of Section 702-Obtained or -Derived Evidence

Defendants also move to suppress the evidence obtained or derived from FISA Section 702 acquisitions. (Doc. No. 146 at 1.) They argue that this evidence should be suppressed because (1) Section 702 violates the Fourth Amendment and (2) the acquisitions here may have violated Section 702's statutory procedures. (*See* Doc. No. 147 at 19–23, 36–37.)

1. Fourth Amendment Argument

Defendants contend that Section 702 acquisitions are unconstitutional because they are subject to, but fail to satisfy, the Fourth Amendment's warrant requirement. (*See* Doc. No. 147 at 19–23.) The warrant requirement, Defendants argue, "presupposes a number of measures that are conspicuously missing from the search and seizure of electronic communications under Section 702": (1) a warrant authorizing the search and seizure; (2) based upon probable cause; (3) describing the place to be searched and the items to be seized with particularity; (4) based on an affidavit under oath or affirmation; (5) issued by a neutral and detached magistrate operating in a judicial capacity; and (6) procedures assuring compliance with the terms of the warrant in its execution. (*Id.* at 23.)

Defendants appear to challenge the constitutionality of Section 702 on its face. (*See* Doc. No. 146 at 1–2; Doc. No. 147 at 19–36.) To succeed on a facial challenge, Defendants would need to establish that no set of circumstances exists under which Section 702 would be valid. *See United States v. Salerno*, 481 U.S. 739, 745 (1987). But in the exercise of judicial restraint, and given that the Government "implemented [the statute] in a defined context" in this case, I will limit Defendants' challenge to an as-applied challenge. *Hasbajrami*, 2016 WL 1029500, at *7 (quoting *In re Directives*, 551 F.3d 1004, 1010 (FISCR 2008)); *see Warshak v. United States*, 532 F.3d 521, 529 (6th Cir. 2008) ("Exercising judicial restraint in a facial challenge frees the Court not only from unnecessary pronouncements on constitutional issues, but also from premature interpretations of statutes in areas where their constitutional application might be cloudy." (quoting *United States v. Raines*, 362 U.S. 17, 22 (1960))).

The Fourth Amendment states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. Const. amend. IV. The Supreme Court, however, has not interpreted the Fourth Amendment to require a warrant, a probable cause determination, or, in fact, any measure of individualized suspicion in every circumstance, for a search to be lawful. *See Nat'l Treasury Emp. Union v. Von Raab*, 489 U.S. 656, 665 (1989); *United States v. Muhtorov*, 187 F. Supp. 3d 1240, 1253 (D. Colo. 2015); *United States v. Mohamud*, No. 3:10-cr-00475, 2014 WL 2866749, at *12 (D. Or. June 24, 2014). And, as critical here, when the Government's actions are "directed against aliens in foreign territory," the Fourth Amendment's protections do not apply. *United States v. Verdugo-Urquidez*, 494 U.S. 259, 267 (1990).

In *Verdugo-Urquidez*, the Supreme Court considered the scope of the Fourth Amendment's protections for non-citizens with no substantial voluntary connection to the United States. *See* 494 U.S. at 261, 264–75. The Court began its analysis in by looking to the text of the Constitution. *Id.* at 264–66. This textual exegesis, the Court noted, suggests that "the people" who enjoy the Fourth Amendment's protections constitute the "class of persons who are a part of a national community or who have otherwise developed sufficient connection with this country to be considered part of that community." *Id.* at 265, 274–75; *see* U.S. Const. amend. IV ("The right of *the people* to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . ." (emphasis added)). Guided by this understanding of the amendment's scope, the Supreme Court concluded that the Fourth Amendment's protections did not apply to the respondent because, "[a]t the time of the search, he was a citizen and resident of Mexico with no voluntary attachment to the United States, and the place searched was located in Mexico." *Verdugo-Urquidez*, 494 U.S. at 274–75.

The Supreme Court supported its holding through an analysis of the drafting history and contemporary views of the Fourth Amendment as well as relevant case law and practical considerations. *Verdugo-Urquidez*, 494 U.S. at 265–74. The drafting history of the Fourth Amendment suggested that its purpose was "to restrict searches and seizures which might be conducted by the United States in domestic matters." *Id.* at 266. And contemporaries of the framers seemed to view the amendment as having no application to the nation's activities "directed against aliens in foreign territory." *Id.* at 267. In earlier cases, the Supreme Court had found that non-citizens enjoyed certain constitutional rights. *Id.* at 270–71. But those cases involved non-citizens who had "come within the territory of the United States and developed substantial connections with [the] country." *Id.* at 271; *see also Johnson v. Eisentrager*, 339 U.S.

763, 770 (1950) (stating that a non-citizen is "accorded a generous and ascending scale of rights as he increases his identity with our society"). The respondent, by contrast, "had no previous significant voluntary connection with the United States." *Verdugo-Urquidez*, 494 U.S. at 271. Practical concerns also favored a narrow scope for the Fourth Amendment's protections. As the Supreme Court noted, "[t]he United States frequently employs Armed Forces outside this country . . . for the protection of American citizens or national security. Application of the Fourth Amendment to those circumstances could significantly disrupt the ability of the political branches to respond to foreign situations involving our national interest." *Id.* at 273–74 (citation omitted). Officials in the executive and legislative branches "are sworn to uphold the Constitution, and they presumably desire to follow its commands. But [a] global view of [the Fourth Amendment's] applicability would plunge them into a sea of uncertainty as to what might be reasonable in the way of searches and seizures conducted abroad." *Id.* at 274.

a. Warrant Requirement

Section 702 surveillance targets non-U.S. persons located outside of the United States. *See* 50 U.S.C. § 1881a(b). But, of course, this does not mean that under Section 702 the Government acquires only foreign communications. If a U.S. person communicates with a targeted individual, the U.S. person's communication will be incidentally acquired. (*See* Doc. No. 191 at 18–20, 30.)

The Fourth Amendment's Protections Do Not Apply to Farooq

Assuming that Farooq was a target of the Section 702 acquisitions, (footnote added)

The identity of the target(s) of the acquisitions is classified. For the purpose of addressing Defendants' argument, this discussion assumes that Farooq was a 702 target.

Defendants contend that under *Verdugo-Urquidez* the Fourth Amendment's protections apply to Farooq because (i) he has substantial connections to the United States and (ii) the acquisitions at issue purportedly occurred on United States soil. If Farooq has substantial connections to the United States, the Fourth Amendment's warrant requirement might apply to the acquisitions at issue and, in turn, the incidental collection of the communication(s) at issue.

The facts regarding Farooq's citizenship and connections to the United States are not in dispute. Farooq is a citizen of India. (*See* Doc. No. 147 at 1.) He was born, however, in the United Arab Emirates ("U.A.E."), where he lived from his birth (in 1978) until 1991. (*Id.*) Farooq came to the United States in August 1999 to attend Louisiana State University ("LSU"). (*Id.*) Farooq studied at LSU through May 2001, when he received a master's degree in electrical engineering. (*Id.*) He then enrolled in an engineering Ph.D. program at Ohio State University ("OSU"). (*Id.*) Farooq remained a student at OSU until August 2004, when he returned to the U.A.E. after his father's death. (*Id.*) Farooq subsequently visited the United States twice (excluding his current presence in the country). He was in the United States on a B-1/B-2 non-immigrant visitor visa from October 26 to November 19, 2007, and from March 18 to April 2, 2008. (Doc. No. 191 at 76.) Farooq made the March 2008 trip to marry his wife, a United States citizen, in Orlando, Florida. (*Id.*; Doc. No. 147 at 8.) Despite his marriage, though, Farooq did not remain in the country. (Doc. No. 191 at 76.)

These facts do not evince a voluntary connection to the United States sufficient to bestow on Farooq the Fourth Amendment's protections. Farooq studied in the United States for roughly five years. But Farooq finished his studies in the United States years before the acquisitions at issue occurred. And after finishing his studies and leaving the United States in 2004, Farooq returned to visit the country only twice in the subsequent years—for around 25 days in 2007 and

for around 16 days in 2008. Although Farooq may have established a sufficient voluntary connection to the United States to avail himself of the Fourth Amendment's protections during his time as a student, Farooq's connection to the United States has weakened over the years. *Cf. Ibrahim v. Dep't of Homeland Sec.*, 669 F.3d 983, 997 (9th Cir. 2012) (concluding that the plaintiff had established a significant voluntary connection to the United States during her four years at Stanford despite a trip abroad during that time because "[t]he purpose of her trip was to further, not to sever, her connection to the United States" and because she "intended her stay abroad to be brief"). A non-citizen's voluntary connection to the United States is not a lifetime status that, once conferred, lasts indefinitely irrespective of the non-citizen's intervening life choices. *Cf. Shaughnessy v. United States ex rel. Mezei*, 345 U.S. 206, 208, 213–15 (1953) (concluding that a 19-month overseas absence of a lawful permanent resident who had previously lived in the United States for 25 years constituted a "clear break in [his] continuous residence here," such that he had no Fifth Amendment right to challenge his denial of re-entry). A voluntary connection is just that—voluntary. Just as a non-citizen can choose to establish a connection with the United States, he can also choose to sever or attenuate that connection. *Cf. id.*; *Ibrahim*, 669 F.3d at 997. By living abroad since his departure from OSU in 2004, and then making only two brief trips to the country in the intervening years, Farooq attenuated the connection to the United States that he may have formed while studying here.

That Farooq's wife is a United States citizen does little to alter the Fourth Amendment analysis. The nationality of Farooq's wife does not automatically amount to a substantial voluntary connection between Farooq and the United States. Farooq's marriage is to an individual, not a nation. Notably, Farooq lived outside the United States despite his marriage to a United States citizen. Farooq came to the United States for the wedding and then promptly left

the country. He remained abroad until he was extradited to the United States to stand trial in this case.

Farooq's second argument for the application of the Fourth Amendment—the location of the Section 702 acquisitions—also falls flat. Farooq argues, based on his knowledge of the logistics of Section 702 collection, that the acquisitions took place in the United States. (Doc. No. 147 at 18 & n.21.) According to Farooq, U.S.-based electronic communications companies are compelled through FISC directives to produce communications to the Government. (*Id.* at 18.) The NSA collects and stores the information in databases located in the United States, and the intelligence agencies, including the NSA, FBI, and CIA, can then query (i.e., search) through the information. (*Id.*)

The Government does not dispute Farooq's assertion that Section 702 acquisition takes place within the United States. (Doc. No. 191 at 37.) The Government argues, instead, that the location of the acquisition is not constitutionally significant in this case. (*Id.*)

The Supreme Court's opinion in *Verdugo-Urquidez* focused primarily on whether the respondent had formed a substantial voluntary connection with the United States. *See* 494 U.S. at 265–75. But the Government's argument—that the location of the search is not constitutionally significant—goes too far. In *Verdugo-Urquidez*, the Court listed the factual circumstances that guided its holding. After noting the respondent was a citizen and resident of Mexico with no voluntary attachment to the United States, the Court noted the place searched was in Mexico. *Id.* at 274–75. Clearly the location of the search has some constitutional significance under *Verdugo-Urquidez*. The question, however, is how much significance the location of the search should carry.

Acquisitions under Section 702 are electronic. This is not a situation, for example, where a non-citizen owns a house in the United States and the Government, claiming the Fourth Amendment does not apply to the non-citizen because he lacks a substantial voluntary connection to the United States, searches the house without first obtaining a warrant and collects incriminating evidence about a U.S. person. I would likely arrive at a different conclusion in that situation. When a search is electronic, the location of the search carries less weight. The more important geographic consideration is the location of the *target* of the acquisition. *See United States v. Mohamud*, 843 F.3d 420, 439 (9th Cir. 2016) ("[A]s one court put it, 'what matters here is the location of the *target*,' and not where the government literally obtained the electronic data." (quoting *Hasbajrami*, 2016 WL 1029500, at *9 n.15)).

A focus on the location of the target better comports with the Supreme Court's statements in *Verdugo-Urquidez* indicating the Fourth Amendment was not intended to apply to Government actions directed against "aliens in foreign territory." 494 at 267. A focus on the location of the target also addresses the Supreme Court's concern that interpreting the Fourth Amendment to protect non-citizens with no substantial voluntary connection with the United States "could significantly disrupt the ability of the political branches to respond to foreign situations involving our national interest." *Id.* at 273–74. Applying Fourth Amendment protections to all electronic acquisitions occurring in the United States would allow numerous aliens in foreign territory, including many suspected terrorists, to claim the protections of the Fourth Amendment. (*See* Gov't Resp. to FISA Section 702 Mot. at 38.)

Focusing on the target's location also conforms to broader Fourth Amendment jurisprudence regarding the reasonable expectation of privacy test and the Supreme Court's repeated admonition that "the Fourth Amendment protects people, not places." *Katz v. United*

States, 389 U.S. 347, 511 (1967); *see, e.g.*, *Minnesota v. Carter*, 525 U.S. 83, 88 (1998) (explaining that the Fourth Amendment "is a personal right that must be invoked by an individual" but that "the extent to which the Fourth Amendment protects people may depend upon where those people are"); *Minnesota v. Olson*, 495 U.S. 91, 96 n.5 (1990) (stating that the Fourth Amendment protects people, not places and "provides sanctuary for citizens wherever they have a legitimate expectation of privacy"); *Smith v. Maryland*, 442 U.S. 735, 740 (1979) ("Consistently with *Katz*, this Court uniformly has held that the application of the Fourth Amendment depends on whether the person invoking its protection can claim a 'justifiable,' a 'reasonable,' or a 'legitimate expectation of privacy' that has been invaded by government action."). The reasonableness of a non-citizen's expectation of privacy regarding his electronic communications typically depends on the location where he makes the communications, not on the location where the United States acquires the communications. *Cf. Carter*, 525 U.S. at 88 ("We have held that 'capacity to claim the protection of the Fourth Amendment depends . . . upon whether the person who claims the protection of the Amendment has a legitimate expectation of privacy in the invaded place.'" (quoting *Rakas v. Illinois*, 439 U.S. 128, 143 (1978))); *United States v. Yonn*, 702 F.2d 1341, 1347 (11th Cir. 1983) ("The location of the electronic equipment does not alter the irrefutable fact that [the defendant] had no justifiable expectation of privacy in his conversation . . . .").

In sum, assuming Farooq was a Section 702 target, he lacked a substantial voluntary connection to the United States at the time of the Section 702 acquisitions sufficient to confer upon him Fourth Amendment protections. That the acquisitions took place in the United States does not alter this conclusion.

i. No Warrant Required

The question, then, is whether the Government needed to obtain a warrant before it incidentally acquired U.S. persons' communications under Section 702 while targeting non-U.S. persons located outside of the United States. Consistent with other courts that have answered this question, and consistent with the Supreme Court's holding in *Verdugo-Urquidez*, I conclude that no warrant was required for the acquisitions in this case. *See Verdugo-Urquidez*, 494 U.S. at 267, 274–74; *Mohamud*, 843 F.3d at 439; *Hasbajrami*, 2016 WL 1029500, at *8–9; *Mohamud*, 2014 WL 2866749, at *14–15. And because no warrant is required, the lack of warrant-related features in Section 702 (i.e., the need for a neutral and detached magistrate to make a probable cause finding and describe the scope of the search with particularity) does not render the statute unconstitutional.

Courts "have long dealt with the issue of incidental interception of non-targeted persons' communications." *Hasbajrami*, 2016 WL 1029500, at *9; *see, e.g.*, *United States v. Kahn*, 415 U.S. 143, 157–58 (1974) (holding that the interception of a wife's conversations on her home telephone was incidental, and not in violation of the Fourth Amendment, because her criminal activities were not foreseen when the Title III wiretap order targeting her husband was obtained); *United States v. Butenko*, 494 F.2d 593, 608 (3d Cir. 1974) (finding warrantless surveillance for foreign intelligence purposes constitutional even though the conversations of United States' citizens would be overheard). As one example, electronic surveillance conducted under FISA Title I incidentally collects the communications of U.S. persons. (*See* Doc. No. 191 at 35–36.) And traditional FISA surveillance, in fact, "is likely to capture a significantly larger concentration of non-targeted U.S. persons' communications than Section 702" because

traditional FISA surveillance does not target only foreign communications. (*See id.* at 36.) Despite this incidental collection, the Sixth Circuit, as well as numerous other courts, have rejected Fourth Amendment challenges to FISA Title I surveillance. *See Damrah*, 412 F.3d at 625. As the FISCR explained in *In re Directives*, "[i]t is settled beyond peradventure that incidental collections occurring as a result of constitutionally permissible acquisitions do not render those acquisitions unlawful." 551 F.3d at 1015; *see also Mohamud*, 843 F.3d at 440 ("The fact that the government knew some U.S. persons' communications would be swept up during foreign intelligence gathering does not make such collection any more unlawful in this context than in the Title III or traditional FISA context."); *Hasbajrami*, 2016 WL 1029500, at *8–9 ("[W]hen surveillance is lawful in the first place—where it is the domestic surveillance of U.S. persons pursuant to a warrant, or the warrantless surveillance of non-U.S. persons who are abroad—the incidental interception of non-targeted U.S. persons' communications with the targeted persons is also lawful." (footnote omitted)). And here, the incidental collection of Defendants' communications did not render unlawful the constitutionally permissible acquisitions targeting non-U.S. persons located outside the United States.

b. Reasonableness

My conclusion that no warrant was required to conduct the Section 702 acquisitions here does not necessarily mean that the Fourth Amendment offers Defendants no protection. Courts considering the constitutionality of Section 702 have assumed the Fourth Amendment offers some protections to the U.S. persons and persons in the United States whose communications have been incidentally collected. *See Mohamud*, 843 F.3d at 441 & n.26.

"Even if a warrant is not required, a search is not beyond Fourth Amendment scrutiny; for it must be reasonable in its scope and manner of execution." *Maryland v. King*, 569 U.S. 435,

448 (2013). Finding that no warrant is required to conduct a search "is merely to acknowledge that 'rather than employing a *per se* rule of unreasonableness, [the court must] balance'" the interests at stake to determine if the search was reasonable. *Id.* (*Illinois v. McArthur*, 531 U.S. 326, 331 (2001)). In balancing the interests, the court examines the totality of the circumstances and weighs, "on the one hand, the degree to which [the search] intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests." *Samson v. California*, 547 U.S. 843, 848 (2006).

As the Supreme Court has explained on various occasions, the Government's interest in protecting the nation from terrorism and foreign threats is an urgent and compelling interest of the highest order. *See, e.g.*, *Holder v. Humanitarian Law Project*, 561 U.S. 1, 28 (2010) ("[T]he Government's interest in combating terrorism is an urgent objective of the highest order."); *Haig v. Agee*, 453 U.S. 280, 307 (1981) ("It is 'obvious and unarguable' that no governmental interest is more compelling than the security of the Nation." (citation omitted)); *see also In re Directives*, 551 F.3d at 1012 ("Here, the relevant governmental interest—the interest in national security—is of the highest order of magnitude."). And acquiring foreign intelligence information through Section 702 is crucial to these national security efforts, the Government argues. (Doc. 191 at 53–54.)

On the other side of the scale are the privacy interests that Defendants and other U.S. persons and persons in the United States have in their electronic communications, both domestic and international. (*See* Doc. No. 147 at 31.) This is not an insignificant interest, the Sixth Circuit suggested in 2010:

> Since the advent of email, the telephone call and the letter have waned in importance, and an explosion of Internet-based communication has taken place. People are now able to send sensitive and intimate information, instantaneously, to friends, family, and colleagues half a world away. . . . Commerce has also

> taken hold in email. Online purchases are often documented in email accounts, and email is frequently used to remind patients and clients of imminent appointment. In short, "account" is an apt word for the conglomeration of stored messages that comprises an email account, as it provides an account of its owner's life. By obtaining access to someone's email, government agents gain the ability to peer deeply into his activities.

Warshak, 631 F.3d at 284.

The Government contends U.S. persons and persons located in the United States have significantly diminished, or nonexistent, privacy interests in communications that "have been transmitted to or obtained from non-U.S. persons located abroad." (Doc. No. 191 at 55.) The Government notes that individuals have no constitutional interest in the communications facilities used by the people targeted under Section 702. (*Id.*) And the Government notes that individuals lack a legitimate expectation of privacy in emails that have already reached their recipient. (*See id.* at 56–57.)

I agree an individual loses some expectation of privacy in an electronic communication after it has reached its recipient. *See Guest v. Leis*, 255 F.3d 325, 333 (6th Cir. 2001) ("[Email users] would lose a legitimate expectation of privacy in an e-mail that had already reached its recipient; at this moment, the e-mailer would be analogous to a letter-writer, whose 'expectation of privacy ordinarily terminates upon delivery' of the letter." (citation omitted)). But the loss is not complete. *See Warshak*, 631 F.3d at 286–87 (holding that "a subscriber enjoys a reasonable expectation of privacy in the contents of emails 'that are stored with, or sent or received through, a commercial ISP'" and neither the ability nor the right of a third-party intermediary to access the contents of a communication is sufficient to extinguish a reasonable expectation of privacy (citation omitted)). An individual still retains a limited expectation of privacy in his electronic communications after the communication has reached its recipient. *See Muhtorov*, 187 F. Supp. 3d at 1255.

When this limited expectation of privacy in delivered electronic communications is weighed against the Government's interest in acquiring foreign intelligence information through Section 702, the Government's interest prevails. And it prevails in large part because the statutory safeguards and procedures required of the Government to convince me the acquisition here was reasonable. Under Section 702: the DNI and the Attorney General must certify that targeting and minimization procedures are in place to protect the privacy of persons located in the United States; the Government's certification, targeting procedures, and minimization procedures are all subject to FISC review; 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"; a significant purpose of the collection must be to obtain foreign intelligence information; minimization procedures limit how long information concerning U.S. persons can be retained and how it can be disseminated; and the DNI and the Attorney General must periodically assess the Government's compliance with the targeting procedures, the minimization procedures, and with the relevant compliance guidelines. (*See* Doc. No. 191 at 58–73.)

When viewed under the totality of the circumstances, I find the Section 702 acquisitions here were reasonable and did not violate the Fourth Amendment.

2. Statutory Argument

Defendants next ask for suppression of the evidence obtained or derived from Section 702 acquisitions because, they argue, the acquisitions may have violated Section 702's statutory procedures. I have carefully reviewed the FISA Section 702 materials submitted by the

Government. And based on that ex parte, in camera review, I conclude that all the statutorily-required procedures were followed here. Defendants' request for suppression of the Section 702 materials is, accordingly, denied.

I now consider Defendants' request for notice and disclosure regarding surveillance techniques (Doc. No. 131).

IV.

In a motion aimed broadly at all the Government's surveillance, Defendants request notice of (1) each surveillance technique the Government used to obtain information about his communications or activities, (2) the timing or duration of each surveillance technique, (3) the legal authority the Government relied upon in conducting the surveillance, and (4) the evidence obtained or derived from each surveillance technique. (Doc. No. 131 at 1.) Defendants propose the Government may have surveilled them using a variety of means and authorizations, including FISA, FAA, Executive Order 12333, the Warrantless Wiretapping Program (also known as the Terrorist Surveillance Program), and National Security Letters. (*Id.* at 2–6.)

A. Due Process

Defendants begin by arguing the Constitution's due process protections mandate the Government's disclosure of the requested information. (*See* Doc. No. 131 at 11–13.) None of the cases cited by Defendants stand for that proposition though.

In *United States v. United States Dist. Court (Keith)*, 407 U.S. 297, 318–24 (1972), for example, the Supreme Court held that the Government must comply with the Fourth Amendment's requirement of prior judicial approval before conducting domestic security surveillance. Because the Government's surveillance in the underlying action was unlawful, the Government was obligated to disclose the impermissibly intercepted conversations to the

defendant. *Id.* at 324. Importantly though, the Supreme Court in *Keith* did not consider the Fourth Amendment considerations associated with *foreign intelligence surveillance*—the surveillance at issue here. *Id.* at 321–22.

In *Jencks v. United States*, 353 U.S. 657, 672 (1957), the Supreme Court held that a criminal action must be dismissed if the Government refuses to comply with an order to produce "relevant statements or reports in its possession of government witnesses touching the subject matter of their testimony at the trial." Defendants, however, request information about surveillance techniques, not statements or reports of Government witnesses.

Berger, *Alderman*, *Kolod*, and *Dalia* and are equally inapposite to Defendants' request. Nowhere in these cases did the Supreme Court establish a broad right to notice of, and information about, each surveillance technique used by the Government. In *Berger*, the Supreme Court found that a New York eavesdrop statute violated the Fourth Amendment because the statute's "blanket grant of permission to eavesdrop [was] without adequate judicial supervision or protective measures." *Berger v. New York*, 388 U.S. 41, 60 (1967). The statute was unconstitutional because, among other reasons, it had no notice requirement and did not "overcome [that] defect by requiring some showing of special facts." *Id.* The Court's conclusion that the statute violated the Fourth Amendment did not, however, suggest that the Constitution's due process provisions grant criminal defendants a right to notice of all surveillance techniques. In *Alderman* and *Kolod*, the Supreme Court outlined the procedures required when the government intends to use evidence from surveillance that, unlike here, has already been deemed unlawful. *See Alderman v. United States*, 394 U.S. 165, 182–83 (1969) (holding that surveillance materials needed to be produced and an adversarial hearing held where the prosecution planned to use evidence from surveillance that had already been deemed unlawful); *Kolod v. United*

States, 390 U.S. 136, 137 (1968) (remanding and directing the district court to hold a hearing where the government admitted that it had conducted unlawful electronic eavesdropping). And in *Dalia*, the Supreme Court rejected the argument that the Fourth Amendment prohibits covert entry onto private premises for the installation of legal electronic bugging equipment. *See United States v. Dalia*, 441 U.S. 238, 246–48 (1979). Addressing this issue in the context of domestic criminal surveillance authorized under Title III of the Omnibus Crime Control and Safe Streets Act of 1968, the Supreme Court noted that Title III provides a constitutionally adequate substitute for advance notice by requiring subsequent notice to those surveilled. *Id.* at 248. The Court did not establish a Constitutional right to notice of all surveillance techniques used to surveil a criminal defendant.

B. Disclosure under 18 U.S.C. § 3504

Defendants also cite 18 U.S.C. § 3504 in support of their request. Under § 3504, if an aggrieved party claims that "evidence is inadmissible because it is the primary product of an unlawful act or because it was obtained by the exploitation of an unlawful act, the opponent of the claim shall affirm or deny the occurrence of the alleged unlawful act." 18 U.S.C. § 3504(a)(1). The statute provides that an "unlawful act" is "any act the use of any electronic, mechanical, or other device . . . in violation of the Constitution or laws of the United States or any regulation or standard promulgated pursuant thereto." *Id.* § 3504(b).

Defendants request notice and information regarding each surveillance technique used by the Government in this case. (*See* Doc. No. 131 at 1, 22.) Defendants' request is undermined, however, by the plain language of § 3504. The statute mandates that the opponent of the unlawful surveillance claim simply "*affirm or deny* the occurrence of the alleged unlawful act." 18 U.S.C. § 3504(a)(1) (emphasis added); *see In re Grand Jury Subpoena (T-112)*, 597 F.3d 189,

200 (4th Cir. 2010) (concluding that the Government satisfied its "obligation to affirm or deny Title III surveillance" where the Government responded to a demand under 18 U.S.C. § 3504(a)(1) by representing that relevant entities "were not and are not a subject of electronic surveillance pursuant to Title III" (internal quotation marks omitted)). The statute does not provide for detailed disclosures regarding each surveillance technique allegedly used by the Government. *See* 18 U.S.C. § 3504(a)(1).

When courts have directed the Government to provide more detailed affirmations or denials under § 3504, they have typically done so only when the aggrieved party's claim is specific, concrete, and relevant. *United States v. Amawi*, 3:06CR719, 2007 WL 1431943, at *1 (N.D. Ohio May 14, 2007). Defendants' claim has none of those characteristics.

Defendants cite *United States v. Alter*, 482 F.2d 1016, 1027 (9th Cir. 1973), in support of the proposition that § 3504 requires more than an affirmation or denial from the Government. In *Alter*, the Government filed an affidavit in response to the appellant's allegations of unlawful surveillance. *Alter*, 482 F.2d at 1027 & n.17. The Ninth Circuit criticized the affidavit for its failure to "squarely . . . affirm or deny" the appellant's allegations. *Id.* at 1027. The affidavit spoke "in conclusory terms," lacked information about the affiant's efforts to investigate the appellant's allegations, failed to explain why the affiant contacted only a limited number of agencies as part of his investigation, and neglected to reveal the dates of claimed surveillance about which the affiant inquired. *Id.* Integral to the Ninth Circuit's discussion, however, was the detailed nature of the appellant's affidavits in which he laid out his allegations of unlawful surveillance. *See id.* ("Alter's affidavits were sufficiently concrete and specific to make a prima facie showing that on the occasions described someone was interfering with his telephone calls and that the F.B.I. was involved."). As the court explained, the Government would only be

obligated to affirm or deny alleged illegal surveillance under § 3504(a) if an aggrieved party first "raise[s] a prima facie issue of electronic surveillance" by revealing through affidavits or other evidence the dates the surveillance alleged took place and the specific facts supporting the party's allegations, among other things. *Id.* at 1026.

But here, unlike in *Alter*, Defendants have not submitted an affidavit or other evidence that makes a prima facie showing of unlawful surveillance. Consequently, even if I were to follow the Ninth Circuit's interpretation of § 3504 as laid out in *Alter*, Defendants would still not be entitled to the information they request.

C. FISA Surveillance

As a subset of their broader request, Defendants ask for additional information about the Government's FISA surveillance. The Government informed Defendants that it intended to offer into evidence, or otherwise use or disclose in the case against them, information obtained or derived from electronic surveillance, physical searches, and acquisitions under FISA Titles I and III and FISA Section 702. (Doc. Nos. 28, 29, 30.) These notices, Defendants argue, are insufficient because they do not provide specific information about each search or seizure conducted by the Government. (*See* Doc. No. 131 at 21.) Defendants request this additional information based on their reading of FISA's text (i.e., 50 U.S.C. §§ 1806(c), 1825(d), 1881e) and legislative history. (*See id.* at 14–21.)

"In all cases of statutory construction, the starting point is the language employed by Congress." *Vergos v. Gregg's Enters., Inc.*, 159 F.3d 989, 990 (6th Cir. 1998) (quoting *Appleton v. First Nat'l Bank of Ohio*, 62 F.3d 791, 801 (6th Cir. 1995)). Where "the statute's language is plain, 'the sole function of the courts is to enforce it according to its terms.'" *United States v. Ron Pair Enters., Inc.*, 489 U.S. 235, 241 (1989) (quoting *Caminetti v. United States*, 242 U.S.

470, 485 (1917)). The Government's notification requirement under FISA Title I (electronic surveillance), FISA Title III (physical searches), and FISA Sections 702 and 703 (acquisitions) reads as follows:

> Whenever the Government intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, against an aggrieved person, any information obtained or derived from [electronic surveillance, a physical search, or an acquisition conducted] pursuant to the authority of this [chapter], the Government shall, prior to the trial, hearing, or other proceeding or at a reasonable time prior to an effort to so disclose or so use that information or submit it in evidence, notify the aggrieved person and the court or other authority in which the information is to be disclosed or used that the Government intends to so disclose or so use such information.

50 U.S.C. § 1806(c); *see id.* §§ 1825(d), 1881e.[6]

Defendants interpret this notice requirement as obligating the Government to inform them of (i) the specific search or seizure events at issue, (ii) the information derived from each event, and (iii) the FISA provision justifying each event. (*See* Doc. No. 131 at 21.) According to Defendants, "Congress's instruction that the government must provide notice prior to each proceeding in which it intends to use or disclose FISA information strongly implies that Congress intended the government to identify the substance of the information." (*Id.* at 16.) Defendants buttress their interpretation by noting Congress also authorized under FISA an aggrieved person's request for suppression on the grounds that "(1) the information was

[6] A similar notice requirement applies to the Government's use of information obtained or derived from a pen register or trap and trace device. 50 U.S.C. § 1845(c). Defendants, however, do not specifically request information about collections made under that title. (*See* Doc. No. 131 at 14–21.) Nor do Defendants cite § 1845(c), the applicable notice requirement. (*See id.*)

FISA does not include a notice requirement regarding information obtained or derived from acquisitions under Section 215 (50 U.S.C. §§ 1861–1864), Section 704 (50 U.S.C. § 1881c), or Section 705 (50 U.S.C. § 1881d). Defendants, in turn, do not specifically request information about acquisitions that may have been made under these sections. (*See* Doc. No. 131 at 14–21.)

unlawfully acquired; or (2) the surveillance was not made in conformity with an order of authorization or approval." (*Id.* (quoting 50 U.S.C. § 1806(e)).)

I disagree with Defendants' reading of the notice requirement. Defendants' interpretation adds three elements to the notice requirement that are found nowhere in the text. The notice requirement is straightforward. It applies to "any information obtained or derived from [electronic surveillance, a physical search, or an acquisition]" that the Government "intends to enter into evidence or otherwise use or disclose [at trial]." 50 U.S.C. § 1806(c); *see id.* §§ 1825(d), 1881e. And it obligates the Government to "notify the aggrieved person . . . *that the Government intends to so disclose or so use such information.*" 50 U.S.C. § 1806(c) (emphasis added); *see id.* §§ 1825(d), 1881e.

Defendants focus on the timing of the required disclosure—"[w]henever the Government intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court." 50 U.S.C. § 1806(c); *see also id.* § 1825(d). But the Government's obligation to provide notice of its intent to use information gathered under FISA "[w]henever the Government intends to enter [it into] evidence or otherwise use or disclose [it]" offers no insight into the content of the required disclosure, and it certainly does not imply that the Government must disclose the specific information about each search or seizure conducted under FISA that Defendants request.

That FISA provides an aggrieved party a statutory basis for suppressing information gathered under its provisions does not support Defendants' interpretation of the notice requirement either. Defendants contend that a lawyer "cannot possibly prepare or file a motion to suppress '*the* evidence obtained or derived from' FISA on the ground that the evidence was unlawfully acquired unless the defendant has notice of *which* information was obtained by FISA,

and the FISA authority under which it was sought." (Doc. No. 131 at 17 (quoting 50 U.S.C. § 1806(e)).) Defendants, however, have done what they claim to be impossible. They have moved to suppress the evidence obtained or derived from FISA Titles I and III and FISA Section 702. Although Defendants' suppression motions were ultimately unsuccessful, their lack of success did not derive from Defendants' inability to prepare or file a suppression motion. Defendants, like others with standing to challenge FISA surveillance, raised their suppression motions based on a Government notice that simply communicated the Government's intent "to offer into evidence, or otherwise use or disclose in any proceedings . . . information obtained or derived from" FISA collections. (*E.g.*, Doc. No. 28.) Defendants, moreover, seem to overlook FISA's actual language regarding motions to suppress. The statute does not require that an aggrieved person identify the challenged evidence with specificity. The statute offers a broad statement of the evidence that an aggrieved person may move to suppress: he "may move to suppress *the evidence obtained or derived from electronic surveillance*." 50 U.S.C. § 1806(e) (emphasis added); *see id.* §§ 1825(f), 1881e.

Given the clarity of the statute, I need not delve into FISA's legislative history. The Government's notice requirement under FISA does not entail anything beyond what the Government has already provided to Defendants.

D. Prior Searches and Seizures

As a further subset of their discovery request, Defendants ask for additional information about the "prior searches and seizures" through which the Government obtained evidence to support its "applications for search warrants under Federal Rule of Criminal Procedure 41." (Doc. No. 131 at 25.) Citing *Franks v. Delaware*, 438 U.S. 154, 155–56 (1978), *Roviaro v. United States*, 353 U.S. 53, 59 (1957), and Federal Rule of Criminal Procedure 16(a)(1)(E)(i),

Defendants seek "information material to determining the legality" of the alleged prior searches and seizures. (Doc. No. 131 at 25.)

None of these authorities substantiates Defendants' request. Under *Franks*, a court will hold an evidentiary hearing to examine the sufficiency of an affidavit supporting a finding of probable cause when the criminal defendant has made a substantial preliminary showing that the affidavit in question contains a false statement which was (1) knowingly or recklessly made and (2) necessary to the finding of probable cause. *See Franks*, 438 U.S. at 155–56, 171–72. Nowhere in *Franks*, however, did the Supreme Court mandate that the Government disclose information about searches and seizures. *See generally id.*

In *Roviaro*, the Supreme Court identified several exceptions to the "informer's privilege"—that is, the Government's ability to withhold from disclosure an informant's identity. The Government's privilege must give way, the Court stated, "[w]here the disclosure of an informer's identity, or of the contents of his communication, is relevant and helpful to the defense of an accused, or is essential to a fair determination of a cause." *Roviaro*, 353 U.S. at 60–61. Because Defendants do not seek to uncover the identity of a Government informant, or obtain the contents of an informant's communication, *Roviaro* lends no support to Defendants' request.

Defendants also bring their request under Federal Rule of Criminal Procedure 16. Information about the alleged prior searches and seizures is purportedly material to preparing a defense, and thus discoverable under Rule 16(a)(1)(E)(i), because Defendants might be able to use the information to suppress evidence obtained pursuant to the Government's subsequent, Rule 41 search warrants. (*See* Doc. No. 131 at 26 ("Evidence obtained pursuant to a search warrant may . . . be suppressed if the affiant relied on evidence obtained or derived from

unlawful government action and the affidavit fails to establish probable cause absent that information.").)

But Defendants read Rule 16(a)(1)(E)(i) too broadly. The Rule only applies to "'shield' claims that 'refute the Government's arguments that the defendant committed the crime charged'" *United States v. Robinson*, 503 F.3d 522, 532 (6th Cir. 2007) (quoting *United States v. Armstrong*, 517 U.S. 456, 462 (1996)). Moreover, under Rule 16(a)(1)(E)(i), information is not material "merely because the government may be able to use it to rebut a defense position." *United States v. Lykins*, 428 F. App'x 621, 624 (6th Cir. 2011) (quoting *United States v. Stevens*, 985 F.2d 1175, 1180 (2d Cir. 1993)). Information is material only if "there [is] an indication that pre-trial disclosure would have enabled the defendant to 'alter the quantum of proof in his favor.'" *Id.* (quoting *Stevens*, 985 F.2d at 1180).

Defendants do not request information about the alleged prior searches and seizures to refute the Government's arguments that they committed the crimes charged (i.e., the Government's case-in-chief). Rather, Defendants request the information because it *might* allow them to move for suppression of unidentified evidence obtained pursuant to subsequent search warrants. (*See* Doc. No. 131 at 26.) Defendants imply that the requested information would alter the quantum of proof in this case. (*See id.*) The connection is too attenuated though. Information about the alleged prior searches and seizures is too disconnected from actually altering the quantum of proof in Defendants' favor for the information to be material under Rule 16(a)(1)(E)(i). *See Lykins*, 428 F. App'x at 624.

Neither *Franks*, *Roviaro*, nor Rule 16(a)(1)(E)(i) entitles Defendants to the discovery they request.

E. CIPA

Lastly, Defendants argue that the Government may not rely on the Classified Information Procedures Act ("CIPA") in refusing to disclose the requested information about its surveillance techniques. (*See* Doc. No. 131 at 24.) In a concurrently issued Memorandum Opinion, however, I have determined that I may review the Government's CIPA § 4 submission in camera and ex parte. And to the extent that the information requested by Defendants may have been addressed in the Government's CIPA § 4 submission, I have already determined the Government may delete that information from the documents to be produced to Defendants through discovery. (*See id.* at 7–8.)

For all of these reasons, I deny Defendants' request for notice and disclosure regarding the Government's surveillance techniques.

V.

Each of Defendants' motions (Doc. Nos. 131, 140, 146, 148, 156) is, accordingly, denied.

So Ordered.

s/ Jeffrey J. Helmick
United States District Judge