IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

UNITED STATES OF AMERICA, *Plaintiff*, v. MOHAMED ELSHINAWY, *Defendant*.	Criminal No. ELH-16-0009

MEMORANDUM OPINION

Mohamed Elshinawy, a United States citizen of Egyptian descent, was indicted on January 13, 2016 (ECF 19) and charged, *inter alia*, with conspiracy to provide and with providing material support to a designated foreign terrorist organization, in the form of personnel, services (including means and methods of communication), and financial services, in violation of 18 U.S.C. §§ 2339B(a)(1) and 2339B(d)(1)(A), (D), (E), and (F). The foreign terrorist organization is ISIS (Islamic State of Iraq and al-Sham or the Islamic State of Iraq and Syria), also known as ISIL (Islamic State of Iraq and the Levant). ECF 19.

In particular, Count One charges conspiracy from in or about February 2015 to December 11, 2015. Count Two charges the substantive offense of providing material support. In Count Three, Elshinawy is charged with the willful collection of funds, "directly and indirectly, with the knowledge that they were to be used, in full or in part, to carry out a terrorist act . . . .", in violation of 18 U.S.C. §§ 2339C(a)(1)(B); 2339C(a)(3).[1] And, Count Four charges the defendant with knowingly and willfully making materially false statements in July 2015, to agents of the Federal Bureau of Investigation ("FBI"), in violation of 18 U.S.C. § 1001(a)(2).

[1] As to Counts Two and Three, defendant is also charged with aiding and abetting under 18 U.S.C. § 2.

The government filed a notice of its intent to offer into evidence information obtained or derived from electronic surveillance and physical search authorized by the United States Foreign Intelligence Surveillance Court ("FISC"), pursuant to the Foreign Intelligence Surveillance Act of 1978 ("FISA"), as amended, 50 U.S.C. §§ 1801-1812. ECF 47. The government subsequently amended its notice, advising of its intent to use only FISA information obtained or derived from electronic surveillance. ECF 81.

Defendant has filed a "Motion To Suppress All Illegally Obtained FISA Evidence And Request For Production Of The Government's FISA Application, Orders, And Related Materials." ECF 63 (the "Motion"). In the Motion, filed pursuant to Fed. R. Crim. P. 12(b)(3)(C) and 50 U.S.C. §§ 1806(e) and 1825(f), defendant seeks disclosure of materials that were presented to the FISC that provided the legal basis for the electronic surveillance from which the government obtained some of the evidence that will be used against defendant. FISA protects such materials from disclosure, except as provided in 50 U.S.C. §§ 1806(f), (g), *i.e.*, where disclosure is necessary for the Court to determine whether the surveillance was legal, or if due process requires disclosure. In the event that disclosure "would pose a threat to national security," defendant asks the Court to "examine the FISA materials and suppress all illegally-obtained material" (ECF 63 at 1) and "to suppress all evidence" not obtained "in conformity with prior authorization or approval." *Id.* at 3.

The government filed a detailed, 52-page unclassified memorandum in opposition to the Motion ("Opposition," ECF 82), as well as a comprehensive classified response and Sealed Appendix (ECF 85), all submitted in camera, ex parte, and under seal. Thereafter, the defendant filed a Reply. ECF 95.

As discussed, *infra*, no hearing is necessary to resolve the Motion. *See also* Local Rule 105.6. For the reasons that follow, I shall DENY the Motion.[2]

I. The Motion

Elshinawy moves to suppress the evidence obtained by the government under FISA (the "FISA Information"), and he seeks disclosure of all FISA applications, orders, and related materials (the "FISA Materials"). ECF 63. Defendant argues in his Reply: "Disclosure of the FISA [M]aterials is necessary to aid the Court in its assessment of the legality of the surveillance, in part, because the surveillance records include a significant amount of non-foreign intelligence, which calls into question whether the Government complied with minimization procedures to limit the acquisition, retention, and dissemination of irrelevant information." ECF 95 at 2. Moreover, defendant asserts: "Defense counsel remains in the dark as to the genesis of the surveillance, whether the Government targeted any other individuals for surveillance in connection with this investigation, and whether the materials disclosed by the Government thus far represent the full scope of surveillance conducted pursuant to FISA . . . or any other authority granting clandestine surveillance of which Mr. Elshinawy was the target." *Id.* at 3. Among other assertions, defendant maintains that any probable cause determination cannot be based on defendant's "First Amendment activities." *Id.* at 9 (citing 50 U.S.C. § 1805(a)(2)(A)). Defendant also contends that the Due Process Clause of the Fifth Amendment compels disclosure of certain FISA evidence, pursuant to 50 U.S.C. § 1806(g). ECF 95 at 10.

[2] Following a hearing in November 2016, I issued a Memorandum Opinion and Order on December 16, 2016 (ECF 83; ECF 84), in which I denied defendant's motion to dismiss the Indictment (ECF 51) and for a severance of Count Four. ECF 52. To the extent relevant, I incorporate from ECF 83 the summary of the allegations and the review of the applicable criminal statutes.

As noted, the government filed an unclassified Opposition in response to the Motion (ECF 82), as well as a classified response. ECF 85. The government included with the Opposition a Declaration and Claim of Privilege executed on November 29, 2016, by then Attorney General Loretta E. Lynch. The Attorney General asserted under oath that disclosure of the government's classified "FISA materials" and an adversary hearing would harm the national security of the United States. *See* ECF 82-1.

Elshinawy's Motion has triggered this Court's review of FISA Materials in order to determine whether the FISA Information was lawfully acquired. *See* 50 U.S.C. §§ 1801-1812. Because the Attorney General filed a Declaration, under oath, representing that disclosure of the classified information would harm the national security of the United States, I conducted an in camera, ex parte review of the FISA Materials relating to the use of electronic surveillance, for the purpose of determining "whether the surveillance of the aggrieved person was lawfully authorized and conducted." 50 U.S.C. § 1806(f).

The Court must determine: (1) whether the certification submitted by the Executive Branch in support of a FISA application(s) was properly made; (2) whether, on de novo review, the application(s) established probable cause, as required by FISA; and (3) whether the collection was properly minimized. *See United States v. Abu-Jihaad*, 630 F.3d 102, 130-31 (2d Cir. 2010); *see also* 50 U.S.C. §§ 1806(f), 1825(g). I am satisfied that these requirements have been met.

The Court must also consider whether the in camera, ex parte review process mandated by 50 U.S.C. § 1806(f) accords with due process. And, the Court must determine whether the FISA submissions contain any information for which disclosure to the defendant is required by due process. *See* 50 U.S.C. § 1806(g). My review reveals that neither of these due process considerations is implicated here.

II. Statutory Framework

FISA, enacted in 1978, created a "secure framework by which the Executive Branch may conduct legitimate electronic surveillance for foreign intelligence purposes within the context of this Nation's commitment to privacy and individual rights." S. Rep. No. 604, 95th Cong., 1st Sess. 15 (1977), reprinted in 1978 U.S. Code Cong. & Ad. News 3904, 3916. "The centerpiece of the legislation" was the creation of the United States Foreign Intelligence Surveillance Court, composed of federal district judges appointed by the Chief Justice. *ACLU Found. of S. California v. Barr*, 952 F.2d 457, 461 (D.C. Cir. 1991) (citing 50 U.S.C. § 1803(a)).

The statute creates a procedure by which the Executive Branch may seek a judicial order from the FISC, authorizing the use of electronic surveillance, physical searches, or both within the United States, where a significant purpose is the collection of foreign intelligence information. 50 U.S.C. §§ 1804(a)(6)(B) and 1823(a)(6)(B).[3] In a criminal prosecution, FISA authorizes the use of information obtained or derived from any FISA-authorized electronic surveillance or physical search, provided, *inter alia*, that advance authorization was obtained from the Attorney General, 50 U.S.C. §§ 1806(b) and 1825(c), and that proper notice is subsequently given to the court and to the aggrieved person against whom the information is to be used. 50 U.S.C. §§ 1806(c)-(d) and 1825(d)-(e).[4]

Upon receiving notice, an aggrieved person against whom the information is to be used may move to suppress the FISA information on the grounds that: (1) the information was

[3] The provisions concerning electronic surveillance and physical searches are quite similar but are contained in separate subchapters of the statute. Subchapter I of FISA concerns the use of electronic surveillance (50 U.S.C. §§ 1801-1813); Subchapter II pertains to physical searches (50 U.S.C. §§ 1821-1829). I have generally provided the parallel citations.

[4] An "aggrieved person" is defined as a person who is the target of an electronic surveillance or the target of a physical search. *See* 50 U.S.C. §§ 1801(k), 1821(2).

unlawfully acquired; or (2) the electronic surveillance and/or physical search was not conducted in conformity with an order of authorization or approval. 50 U.S.C. §§ 1806(e) and 1825(f). In addition, FISA contemplates that a defendant may file a motion or request under any other federal statute or rule to discover or obtain applications, orders, or other materials relating to electronic surveillance or physical searches. 50 U.S.C. §§ 1806(f) and 1825(g).

With the exception of emergency authorizations,[5] FISA requires a prior court order to conduct electronic surveillance or searches in order to gather "foreign intelligence information." *See* 50 U.S.C. §§ 1804(a)(6)(B) and 1823(a)(6)(B). And, as indicated, FISA requires the Attorney General to approve an application submitted to the FISC for the collection of "foreign intelligence information." 50 U.S.C. §§ 1805(a)(1) and 1824(a)(1). Under 50 U.S.C. §§ 1801(e) and 1821(1), "foreign intelligence information" means

[5] The Attorney General may authorize emergency use of electronic surveillance and physical searches if the Attorney General, pursuant to 50 U.S.C. § 1805(e)(1) or 50 U.S.C.§ 1824(e)(1) (alterations added):

> (A) reasonably determines that an emergency situation exists with respect to the employment of electronic surveillance [or physical search] to obtain foreign intelligence information before an order authorizing such surveillance can with due diligence be obtained;
>
> (B) reasonably determines that the factual basis for the issuance of an order under this subchapter to approve such electronic surveillance [or physical search] exists;
>
> (C) informs, either personally or through a designee, a judge having jurisdiction under [50 U.S.C. § 1803, or a judge of the Foreign Intelligence Surveillance Court] at the time of such authorization that the decision has been made to employ emergency electronic surveillance [or physical search]; and
>
> (D) makes an application in accordance with this subchapter to a judge having jurisdiction under section 1803 of this title [or to a judge of the Foreign Intelligence Surveillance Court] as soon as practicable, but not later than 7 days after the Attorney General authorizes such surveillance [or physical search].

> (1) 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;
>
> (B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or
>
> (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or
>
> (2) information with respect to a foreign power or foreign territory 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.

50 U.S.C. § 1801(e); *see also* § 1821(1) (adopting definitions from 50 U.S.C. § 1801).

"United States person," a term referenced above, is defined in 50 U.S.C. § 1801(i). It states, in part, that a "United States person" is "a citizen of the United States, an alien lawfully admitted for permanent residence …, an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power…." *See also* 50 U.S.C. § 1821(2) (adopting the definition in 50 U.S.C. § 1801).

Strict requirements govern an application to conduct electronic surveillance pursuant to FISA. The application must contain information as set forth in 50 U.S.C. § 1804(a)(1)-(9), as follows:

> (1) the identity of the Federal officer making the application;

(2) the identity, if known, or a description of the specific target of the electronic surveillance;

(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 is a foreign power or an agent of a foreign power; and

(B) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by 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 surveillance;

(6) a certification or certifications by the Assistant to the President for National Security Affairs, an executive branch official or officials designated by the President from among those executive officers employed in the area of national security or defense and appointed by the President with the advice and consent of the Senate, or the Deputy Director of the Federal Bureau of Investigation, if designated by the President as a certifying official--

(A) that the certifying official deems the information sought to be foreign intelligence information;

(B) that a significant purpose of the surveillance is to obtain foreign intelligence information;

(C) that such information cannot reasonably be obtained by normal investigative techniques;

(D) that designates the type of foreign intelligence information being sought according to the categories described in section 1801(e) of this title; 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 surveillance;
>
> (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 action taken on each previous application; and
>
> (9) a statement of the period of time for which the electronic surveillance is required to be maintained, and if the nature of the intelligence gathering is such that the approval of the use of electronic surveillance under this subchapter should not automatically terminate when the described type of information has first been obtained, a description of facts supporting the belief that additional information of the same type will be obtained thereafter.

An application to conduct a physical search pursuant to FISA must contain similar information. In addition, it must include a statement of the facts and circumstances that justify the applicant's belief that "the premises or property to be searched contains foreign intelligence information" and that each "premises or property to be searched is or is about to be, owned, used, possessed by, or is in transit to or from" the target. 50 U.S.C. §§ 1823(a)(3)(B), (C).

As mentioned, an application to the FISC for a FISA order must include a certification from a high-ranking executive branch official. That official must have national security responsibilities and must indicate, designate, or include:

> (A) that the certifying official deems the information sought to be foreign intelligence information;
>
> (B) that a significant purpose of the surveillance is to obtain foreign intelligence information;
>
> (C) that such information cannot reasonably be obtained by normal investigative techniques;
>
> (D) that designates the type of foreign intelligence information being sought according to the categories described in [50 U.S.C. § 1801(e)]; and
>
> (E) … 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.

50 U.S.C. § 1804(a)(6)(A)-(E); *see also* 50 U.S.C. § 1823(a)(6).

The FISC may approve the application for electronic surveillance, physical searches, or both, only upon finding, among other things, that: (1) the application has been made by a "Federal officer" and has been approved by the Attorney General; (2) there is probable cause to believe that (A) the target of the electronic surveillance and/or physical search is a foreign power or an agent of a foreign power, and that (B) the facilities or places at which the electronic surveillance is directed are being used, or are about to be used, by a foreign power or an agent of a foreign power (or that the premises or property to be searched 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); (3) the proposed minimization procedures meet the statutory requirements set forth in 50 U.S.C. § 180l(h) (electronic surveillance) and 50 U.S.C. § 1821(4) (physical search); (4) the application contains all of the statements and certifications required by Section 1804 or Section 1823; and (5) if the target is a United States person, that the certifications are not clearly erroneous. *See* 50 U.S.C. §§ 1805(a)(1)-(4) and § 1824(a)(l)-(4).

As noted, an application must establish probable cause to believe that the target is a foreign power or an agent of a foreign power. FISA defines "foreign power" in 50 U.S.C. § 1801(a)(1)-(7), as follows:

> (1) a foreign government or any component, thereof, whether or not recognized by the United States;
>
> (2) a faction of a foreign nation or nations, not substantially composed of United States persons;

> (3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments;
>
> (4) a group engaged in international terrorism or activities in preparation therefor;
>
> (5) a foreign-based political organization, not substantially composed of United States persons;
>
> (6) an entity that is directed and controlled by a foreign government or governments; or
>
> (7) an entity not substantially composed of United States persons that is engaged in the international proliferation of weapons of mass destruction.

S*ee also* 50 U.S.C. § 1821(1) (adopting definitions from 50 U.S.C. § 1801).

"Agent of a foreign power" is defined in 50 U.S.C. § 1801(b)(1) and (2), as follows:

> (1) any person other than a United States person, who--
>
> > (A) acts in the United States as an officer or employee of a foreign power, or as a member of a foreign power as defined in subsection (a)(4) of this section, irrespective of whether the person is inside the United States;
> >
> > (B) acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances indicate that such person may engage in such activities, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities;
> >
> > (C) engages in international terrorism or activities in preparation therefore [sic];
> >
> > (D) engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor; or
> >
> > (E) engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor, for or on behalf of a foreign power, or knowingly aids or abets any person in the conduct of such proliferation or activities in preparation therefor, or knowingly conspires with any person to engage in such proliferation or activities in preparation therefor; or
>
> (2) any person who--

> (A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States;
>
> (B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;
>
> (C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power;
>
> (D) knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power; or
>
> (E) knowingly aids or abets any person in the conduct of activities described in subparagraph (A), (B), or (C) or knowingly conspires with any person to engage in activities described in subparagraph (A), (B), or (C).

50 U.S.C. §§ 1801(b)(l) and (2); *see also* 50 U.S.C. § 1821(1) (adopting definitions from 50 U.S.C. § 1801).

Notably, FISA specifies that no United States person may be considered a foreign power or an agent of a foreign power solely on the basis of activities protected by the First Amendment to the Constitution. 50 U.S.C. §§ 1805(a)(2)(A) and 1824(a)(2)(A). Although protected First Amendment activities cannot form the sole basis for FISA-authorized electronic surveillance or physical searches, they may be considered by the FISC if there is other activity indicating that the target is an agent of a foreign power. *United States v. Rosen,* 447 F. Supp. 2d 538, 549-50 (E.D. Va. 2006); *United States v. Rahman,* 861 F. Supp. 247, 252 (S.D.N.Y. 1994), *aff'd,* 189 F. 3d 88 (2d Cir. 1999).

If the FISC has made all of the necessary findings and is satisfied that the FISA application meets the required statutory provisions, the FISC issues an ex parte order authorizing the requested electronic surveillance, physical searches, or both. 50 U.S.C. §§ 1805(a) and

1824(a). Pursuant to the applicable statutes, the FISA order must specify: (1) the identity, if known, or a description of the specific target of the collection; (2) the nature and location of each facility or place at which the electronic surveillance will be directed or of each of the premises or properties that will be searched; (3) the type of information sought to be acquired and the type of communications or activities that are to be subjected to the electronic surveillance, or the type of information, material, or property that is to be seized, altered, or reproduced through the physical search; (4) the manner and means by which electronic surveillance will be effected and whether physical entry will be necessary to effect that surveillance, or a statement of the manner in which the physical search will be conducted; (5) the period of time during which electronic surveillance is approved and/or the authorized scope of each physical search; and (6) the applicable inimization procedures. *See* 50 U.S.C. §§ 1805(c)(l) and 2(A) and 50 U.S.C. §§ 1824(c)(l) and 2(A).[6]

When a defendant moves to suppress FISA Information under 50 U.S.C. §§ 1806(e) or 1825(t), or seeks to discover the FISA Materials, federal courts, including the Fourth Circuit, have ruled that FISA anticipates an ex parte, in camera determination as "the rule," with disclosure and an adversary hearing "the exception, occurring *only* when necessary." *United States v. Squillacote*, 221 F.3d 542, 554 (4th Cir. 2000) (quoting *United States v. Belfield*, 692 F.2d 141, 147 (D.C. Cir. 1982)) (emphasis in original; internal quotations omitted); *see United States v. El-Mezain*, 664 F.3d 467, 567 (5th Cir. 2011) ("'[D]isclosure of FISA materials is the exception and *ex parte, in camera* determination is the rule.'") (quoting *Abu-Jihaad*, 630 F.3d 102 at 129); *see also United States v. Omar*, 786 F.3d 1104, 1111 (8th Cir. 2015); *United States*

[6] Under FISA, electronic surveillance or physical searches targeting a United States person may be approved for up to ninety days. However, a non-United States person may be subject to the surveillance for up to 120 days. 50 U.S.C. §§ 1805(d)(l) and 1824(d)(l).

v. Isa, 923 F.2d 1300, 1306 (8th Cir. 1991); *United States v. Duggan*, 743 F.2d 59, 78 (2d Cir. 1984); *United States v. Nicholson*, No. 09-CR-40-BR, 2010 WL 1641167, at *3-4 (D. Or. Apr. 21, 2010); *Rosen*, 447 F. Supp. 2d at 546; *United States v. Spanjol*, 720 F. Supp. 55, 59 (E.D. Pa. 1989), *aff'd*, 958 F.2d 365 (3d Cir. 1992).

As the government points out, ECF 82 at 26, the legality of FISA's in camera, ex parte review provisions has been upheld by virtually every federal court that has considered the matter. *See, e.g., El-Mezain*, 664 F.3d at 567; *Abu-Jihaad*, 630 F.3d at 117; *see United States v. Damrah*, 412 F.3d 618, 624 (6th Cir. 2005) ("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."); *Barr*, 952 F.2d at 462 (recognizing that federal district courts "'shall' conduct *ex parte, in camera* reviews to determine whether FISA surveillance, undertaken pursuant to an order of the FISA Court, was 'lawfully authorized and conducted' . . . .") (citation omitted) and *id.* at 465 (upholding lack of adversary hearing, and recognizing that the procedure in § 1806(f) is "an acceptable means" to adjudicate constitutional rights); *Isa*, 923 F.2d at 1306-07 (upholding as constitutional the district court's in camera, ex parte review); *United States v. Ott*, 827 F.2d 473, 476-77 (9th Cir. 1987) (recognizing that FISA's review procedures do not deprive a defendant of due process); *Belfield*, 692 F.2d at 148-49; *United States v. Gowadia*, No. CR. 05-00486 HG-KSC, 2009 WL 1649714, at *2 (D. Haw. June 8, 2009); *United States v. Warsame*, 547 F. Supp. 2d 982, 988-89 (D. Minn. 2008); *United States v. Jayyousi*, No. 04-60001-CR, 2007 WL 851278, at *7-8 (S.D. Fla. Mar. 15, 2007); *United States v. Nicholson*, 955 F. Supp. 582, 592 (E.D. Va. 1997); *Spanjol*, 720 F. Supp. at 58-59; *see also United States v. Benkahla*, 437 F. Supp. 2d 541, 554 (E.D. Va. 2006) (rejecting defendant's claim that in camera, ex parte review would violate his Fifth Amendment right to due process and Sixth Amendment right to counsel); *United States*

v. Megahey, 553 F. Supp. 1180, 1194 (E.D.N.Y. 1982) ("*ex parte, in camera* procedures provided in 50 U.S.C. § 1806(f) are constitutionally sufficient to determine the lawfulness of the electronic surveillance at issue while safeguarding defendants' fourth amendment rights"), *aff'd without opinion*, 729 F.2d 1444 (2d Cir. 1983), and *aff'd sub nom. Duggan*, *supra*, 743 F.2d 59 (1984); *United States v. Falvey*, 540 F. Supp. 1306, 1315 (E.D.N.Y. 1982) (a "massive body of pre-FISA case law of the Supreme Court, this Circuit and others" supports the conclusion "that the legality of electronic surveillance should be determined on an in camera, ex parte basis").

On the filing of the Attorney General's Declaration, such as was filed here, the court "may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials" relating to the surveillance or physical search only "where such disclosure is necessary to make an accurate determination of the legality of the surveillance or search." 50 U.S.C. §§ 1806(f), 1825(g). Such disclosures should occur "'only 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 misrepresentations 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.'" *Rosen,* 447 F. Supp. 2d at 546 (quoting *Belfield,* 692 F.2d at 147) (internal quotation marks omitted).

III. Discussion

A.

At the outset, I am satisfied that the in camera, ex parte review process contemplated by FISA accords with due process under the Constitution. *See* cases cited, *supra,* at pages 14-15,

including, *e.g.*, *El-Mezain*, 664 F.3d at 567; *Abu-Jihaad*, 630 F.3d at 117; *Damrah*, 412 F.3d at 624; *Ott*, 827 F.2d at 476-77; *United States v. Butenko*, 494 F.2d 593, 607 (3d Cir. 1974); *Warsame*, 547 F. Supp. 2d at 988-89; *Benkahla*, 437 F. Supp. 2d at 554 (rejecting defendant's claim that *in camera, ex parte* review violates his Fifth Amendment right to due process and Sixth Amendment right to counsel); *Spanjol*, 720 F. Supp. at 58-59.

Due Process does not require the Court to provide the defendant with access to the FISA Materials, except as provided in 50 U.S.C. §§ 1806(f), (g). *See, e.g., Nicholson,* 955 F. Supp. at 592 (finding, based on "'the unanimous holdings of prior case law ... that FISA does not violate the Fifth or Sixth Amendments by authorizing *ex parte in camera* review'") (internal citation omitted); *see El-Mezain,* 664 F.3d at 567; *Abu-Jihaad,* 630 F.3d at 117-131; *Damrah,* 412 F.3d at 624; *Barr*, 952 F.2d at 465; *Ott,* 827 F.2d at 476-77; *Belfield*, 692 F.2d at 148-49; *Nicholson,* 2010 WL 1641167, at *3-4; *Gowadia,* 2009 WL 1649714, at *2; *Jayyousi,* 2007 WL 851278, at *7-8; *Benkahla*, 437 F. Supp. 2d at 554; *Spanjol*, 720 F. Supp. at 58-59; *Megahey*, 553 F. Supp. at 1194-95; *Falvey*, 540 F. Supp. at 1315-16;

Moreover, there is no basis for disclosure of the FISA Materials pursuant to 50 U.S.C. § 1806(g). Under § 1806(g), such disclosure is only permitted if this Court's in camera, ex parte review establishes that "due process requires discovery or disclosure." The plain intention of § 1806(g)—allowing the Court to order disclosure of materials to which the defendant would be entitled under the Due Process Clause, such as material under *Brady v. Maryland,* 373 U.S. 83 (1963)—does not support the defendant's request for access to the FISA Materials.

B.

When a defendant moves to suppress FISA Information or seeks disclosure of FISA Materials the request is evaluated using FISA's probable cause standard. *See, e.g., United States*

v. Pelton, 835 F.2d 1067, 1075 (4th Cir. 1987); *see also United States v. Duka,* 671 F.3d 329, 336-37 (3d Cir. 2011) (rejecting appellant's challenge to FISA's probable cause standard because it does not require any indication that a crime has been committed); *El-Mezain,* 664 F.3d at 564. In the Fourth Circuit, the district judge conducts a *de* novo review of the FISC's probable cause determination. *See United States v. Hassan,* 742 F.3d 104, 138-39 (4th Cir. 2014) (noting that the district court "articulated and correctly applied the principles established by FISA and our precedent, reviewing the FISA materials *'de novo* with no deference accorded to the ... probable cause determinations, but with a presumption of validity accorded to the certifications"') (quoting district court opinion); *United States v. Hammoud,* 381 F.3d 316, 332 (4th Cir. 2004), *rev'd on other grounds,* 543 U.S. 1097 (2005), *reinstated in pertinent part,* 405 F.3d 1034 (4th Cir. 2005); *United States v. Kashmiri,* No. 09 CR 830–4, 2010 WL 4705159 at *1 (N.D. Ill. Nov. 10, 2010); *Rosen,* 447 F. Supp. 2d at 545.[7]

FISA requires a finding of probable cause that the target is a foreign power or an agent of a foreign power and that each facility or place at which the electronic surveillance or physical search is directed is being used, or is about to be used, or that the property or premises to be searched 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 Omar,* 786 F.3d at 1111 ("'[R]ather than focusing on probable cause to believe that a person has committed a crime, the FISA standard focuses on the status of the target as a foreign power or an agent of a foreign power.'") (quoting *El-Mezain,* 664 F.3d at *564*); *Duka,* 671 F.3d at 338; *Abu-Jihaad,* 630 F.3d at 130-31; *United States v.*

[7] Other courts have afforded deference to the findings of the FISC. *Abu-Jihaad,* 630 F.3d at 130; *accord United States v. Ahmed,* No. 1:06-CR-147-WSD-GGB, 2009 U.S. Dist. Lexis 120007, at *21-22 (N.D. Ga. Mar. 19, 2009) (FISC's "determination of probable cause should be given 'great deference' by the reviewing court") (citing *Illinois v. Gates,* 462 U.S. 213, 236 (1983)).

Cavanagh, 807 F.2d 787, 790 (9th Cir. 1987) (citing *United States v. United States District Court*, 407 U.S. 297, 322 (1972)).

This probable cause standard "reflects the purpose for which FISA search orders are issued." *United States v. Ahmed*, No. 1:06-CR-147-WSD-GGB, 2009 U.S. Dist. Lexis 120007, at *22 (N.D. Ga. Mar. 19, 2009)[8]; *see United States v. Ning Wen*, 477 F.3d 896, 898 (7th Cir. 2007) (holding that FISA is constitutional despite using "a definition of 'probable cause' that does not depend on whether a domestic crime has been committed"); *Damrah*, 412 F.3d at 625 (denying the defendant's claim that FISA' s procedures violate the Fourth Amendment); *In re Sealed Case*, 310 F.3d 717, 738, 746 (FISA Ct. Rev. 2002) (stating that while many of FISA's requirements differ from those in Title III, few of those differences have constitutional relevance); *Pelton*, 835 F.2d at 1075 (finding FISA's procedures compatible with the Fourth Amendment); *Cavanagh*, 807 F.2d at 790-91 (holding that FISA satisfies the Fourth Amendment requirements of probable cause and particularity); *Duggan*, 743 F.2d at 74 (concluding that FISA does not violate the Fourth Amendment); *Warsame*, 547 F. Supp. 2d at 993-94 (recognizing that FISA's probable cause and particularity requirements satisfy the reasonableness requirement of the Fourth Amendment); *United States v. Mubayyid*, 521 F. Supp. 2d 125, 135-41 (D. Mass. 2007) (rejecting claim that FISA violates the Fourth Amendment's judicial review, probable cause, notice, and particularity requirements); *Falvey*, 540 F. Supp. at 1311-14 (finding that FISA procedures satisfy the Fourth Amendment's warrant requirement).

I have made a *de novo* review of the FISC's probable cause determinations, without according deference to the FISC's findings. *See Hassan*, 742 F.3d at 138-139. In my view, the FISA Materials readily meet FISA's probable cause standard and the requirements of the Fourth

[8] The Court could not locate a Westlaw citation for this case.

Amendment to the United States Constitution. *See, e.g.*, *El-Mezain*, 664 F.3d at 568-70; *Abu-Jihaad*, 630 F.3d at 117-19; *Isa*, 923 F.2d at 1304; *Cavanagh*, 807 F.2d at 790-91 (ruling that Fourth Amendment's probable cause and particularity requirements are satisfied for an order targeting a facility used by a foreign power). FISA's "significant purpose" standard is also constitutional under the Fourth Amendment. *See Duka*, 671 F.3d at 343-45.

C.

As to the certifications submitted in support of a FISA application, they are "subjected only to minimal scrutiny by the courts," *United States v. Badia*, 827 F.2d 1458, 1463 (11th Cir. 1987), and are to be presumed valid. *See Hassan*, 742 F.3d at 138-39 (stating that district court correctly reviewed materials with "a presumption of validity accorded to the certifications") (internal quotes and citations omitted); *see also Pelton*, 835 F.2d at 1076 ("Where ... the statutory application was properly made and earlier approved by a FISA judge, it carries a strong presumption of veracity and regularity in a reviewing court."); *Abu-Jihaad*, 630 F.3d at 130 ("FISA warrants are subject to 'minimal scrutiny by the courts,' both upon initial presentation and subsequent challenge" and "'the representations and certifications ... should be presumed valid' by a reviewing court absent a showing sufficient to trigger a *Franks* hearing.") (quoting *Duggan*, 743 F.2d at 77 & 77 n.6); *United States v. Campa*, 529 F.3d 980, 993 (11th Cir. 2008) ("The reviewing court has no greater authority to review the certifications of the executive branch than the FISA court has."); *United States v. Sherifi*, 793 F. Supp. 2d 751, 760 (E.D.N.C. 2011). When a FISA application is presented to the FISC, "[t]he FISA judge, in reviewing the application, is not to second-guess the executive branch official's certification that the objective of the surveillance is foreign intelligence information." *Duggan*, 743 F.2d at 77; *see also id.* at 77 n.6 (citing *Franks v. Delaware*, 438 U.S. 154, 171 (1978)); *Sherifi*, 793 F. Supp. 2d at 760 ("a

presumption of validity [is] accorded to the certifications"); *Nicholson*, 2010 WL 1641167, at *5; *Warsame*, 547 F. Supp. 2d at 990; *Campa*, 529 F.3d at 993; *Rosen*, 447 F. Supp. 2d at 545.

On review, the district court must determine whether the certifications were made in accordance with FISA's requirements. *See United States v. Alwan*, No. 1:11-CR-13-R, 2012 WL 399154, at *7 (W.O. Ky. Feb. 7, 2012) ("'The [c]ourt is not to second-guess whether the certifications were correct, but merely to ensure they were properly made.'") (*quoting Ahmed*, 2009 U.S. Dist. LEXIS 120007, at *20) (alteration in *Alwan*). If the target is a United States person, then the district court should also ensure that each certification is not "clearly erroneous." *Campa*, 529 F.3d at 994; *Duggan*, 743 F.2d at 77; *Kashmiri*, 2010 WL 4705159 at *2. A certification is clearly erroneous when "the reviewing court . . . is left with the definite and firm conviction that a mistake has been committed." *United States v. U.S. Gypsum Co.*, 333 U.S. 364, 395 (1948); *see United States v. Garcia*, 413 F.3d 201, 222 (2d Cir. 2005); *United States v. Islamic American Relief Agency ("IARA")*, No. 07-00087-CR-W-NKL, 2009 WL 5169536, at *4 (W.D. Mo. Dec. 21, 2009).

The certifications here were made in accordance with FISA's requirements. Further, defendant provides no facts in support of a claim that he was considered a foreign power solely upon the basis of activities protected by the First Amendment. The Court may consider a U.S. person's First Amendment activities provided that they are not the sole basis for authorizing electronic surveillance. *See* 50 U.S.C. § 1805(a)(2)(A); *Rosen*, 447 F.Supp.2d at 549-50 (stating that even activities that fall within the purview of the First Amendment's protection may be considered by the Court if other activity is indicative that the target is an agent of a foreign power). Furthermore, not all speech falls within the protection of the First Amendment;

statements made in furtherance of a conspiracy may be evidence of the participant's criminal intent.

D.

If a reviewing court is satisfied that the electronic surveillance was properly certified and that the information was lawfully acquired pursuant to FISA, it must then examine whether the electronic surveillance was lawfully conducted. *See* 50 U.S.C. § 1806(e)(2). In order to examine whether the electronic surveillance was lawfully conducted, the reviewing court must determine whether the government followed the relevant minimization procedures as to information acquired pursuant to FISA.

In reviewing the adequacy of minimization efforts, the court must make an "objective assessment of the [agents'] actions in light of the facts and circumstances confronting [them] at the time." *Scott v. United States*, 436 U.S. 128, 136 (1978). With respect to FISA, the Fourth Circuit has said: "The minimization requirement obligates the Government to make a good faith effort to minimize the acquisition and retention of irrelevant information." *Hammoud,* 381 F.3d at 334; *see also Mubayyid,* 521 F. Supp. 2d at 135; *IARA,* 2009 WL 5169536, at *6 ("'the Court's role is to determine whether on the whole, the agents have shown a high regard for the right of privacy and have done all they reasonably could do to avoid unnecessary intrusion'") (quoting Senate Report at 39-40) (internal quotations marks and citation omitted); *Rosen,* 447 F. Supp. 2d at 550-551 (quoting Senate Report at 39).

Moreover, the government is not required to minimize information that is "evidence of a crime," whether or not it is also foreign intelligence information. 50 U.S.C. §§ 1801(h)(3), 1821(4)(c); *see also Isa,* 923 F.2d at 1304 (noting that "[t]here is no requirement that the 'crime' be related to foreign intelligence"). As a result, to the extent that certain communications of a

United States person may be evidence of a crime or otherwise may establish an element of a substantive or conspiratorial offense, such communications need not be minimized. *Id.* at 1305.

E.

As noted, disclosure is within the Court's discretion following ex parte, in camera review, but only if the court is unable to determine the legality of the electronic surveillance without the assistance of defense counsel. 50 U.S.C. §§ 1806(f), 1825(g). *See Daoud,* 755 F.3d at 482; *Duggan,* 743 F .2d at 78; *Rosen,* 447 F. Supp. 2d at 546. The Fourth Circuit has "emphasized that, where the documents 'submitted by the government [are] sufficient' to 'determine the legality of the surveillance,' the FISA materials should not be disclosed." *Hassan,* 742 F.3d at 138 (quoting *Squillacote,* 221 F.3d at 554). In this case, the FISA Materials are clear and well-organized and more than adequate to enable me to resolve the defendant's Motion.

Based on my review of the FISA submissions, I am satisfied that I do not require the assistance of the defense to make an accurate determination of the legality of the electronic surveillance. Therefore, there is no valid basis for disclosure of any of the FISA Materials to the defendant. *See Duggan*, 743 F.2d at 78 (holding that disclosure should occur "only if [the court] decides that such disclosure is 'necessary to make an accurate determination of the legality of the surveillance'") (quoting 50 U.S.C. § 1806(f)).

F.

I conclude that the government satisfied FISA's requirements to obtain an order(s) for electronic surveillance; that the information obtained pursuant to FISA was lawfully acquired; and that the electronic surveillance was made in conformity with an order(s) of authorization or approval. Moreover, the defense has failed to present a valid basis for disclosure of FISA Materials.

III.

Upon review, in camera and ex parte, of the relevant FISA Materials contained in the Sealed Appendix submitted to the Court by the government, in conjunction with the government's classified response, the Court finds as follows:

1. In accordance with 50 U.S.C. § 1805(a)(1), the application(s) was/were made by a federal officer and approved by the Attorney General;

2. In accordance with 50 U.S.C. § 1805(a)(2)(A), the application(s) contained facts establishing probable cause to believe that the target of the electronic surveillance was an agent of a foreign power;

3. In accordance with 50 U.S.C. § 1805(a)(2)(A), no United States person was determined to be an agent of a foreign power solely upon the basis of activities protected by the First Amendment to the United States Constitution;

4. In accordance with 50 U.S.C. § 1805(a)(2)(B), the application(s) made pursuant to 50 U.S.C. § 1804 contained facts establishing probable cause to believe that each of the facilities or places at which the electronic surveillance was directed was being used, or was about to be used, by a foreign power or an agent of a foreign power;

5. In accordance with 50 U.S.C. § 1805(a)(3), the minimization procedures incorporated into the application(s) and order(s) met the requirements of 50 U.S.C. § 1801(h), and the government implemented such minimization procedures in conformity with an order of authorization or approval;

6. In accordance with 50 U.S.C. § 1805(a)(4), the application(s) contained all of the statements and certifications required by 50 U.S.C. § 1804;

7. In accordance with 50 U.S.C. § 1805(a)(4), no certification in an application for a target who was a United States person was clearly erroneous on the basis of the statement made pursuant to 50 U.S.C. § 1804(a)(6)(E) or any other information furnished under 50 U.S.C. § 1804(c);

8. In accordance with 50 U.S.C. § 1804(a)(6)(B), a "significant purpose" of the government's collection pursuant to FISA was to obtain foreign intelligence information;

9. The order(s) issued by the FISC satisfied the requirements of 50 U.S.C. § 1805(c);

10. The order(s) issued by the FISC satisfied the requirements of 50 U.S.C. § 1805(d);

11. Disclosure to the defense of the FISA Materials is not required because the Court was able to make an accurate determination of the legality of the electronic surveillance without disclosing the FISA Materials or any portions thereof; and

12. Due process does not otherwise require disclosure of the FISA Materials to the defendant.

Date: March 20, 2017

/s/
Ellen L. Hollander
United States District Judge