UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,	:	
-*v.*-	:	
	:	17 Cr. 779 (LAP)
CHI PING PATRICK HO, a/k/a "Patrick C. P. Ho," a/k/a "He Zhiping,"	:	
Defendant.	:	

THE GOVERNMENT'S UNCLASSIFIED MEMORANDUM OF LAW IN OPPOSITION TO THE DEFENDANT'S MOTION TO SUPPRESS AND FOR DISCLOSURE OF FISA MATERIALS

GEOFFREY S. BERMAN
United States Attorney
Southern District of New York
Attorney for the United States of America

Daniel C. Richenthal
Andrew DeFilipis
Assistant United States Attorneys

Kim Robbins-Segers
Patrick Murphy
Attorneys
National Security Division
United States Department of Justice

UNCLASSIFIED TABLE OF CONTENTS

TABLE OF AUTHORITIES

FEDERAL CASES

U.S. CONSTITUTION

FEDERAL STATUTES

OTHER AUTHORITIES

I. INTRODUCTION

The Government respectfully submits this unclassified memorandum of law in opposition to the motion of Chi Ping Patrick Ho (Ho or the defendant) to suppress and for disclosure of Foreign Intelligence Surveillance Act (FISA) Materials (the Motion). Ho's Motion seeks (1) suppression of all evidence obtained or derived under FISA (FISA information); and (2) disclosure of the FISA application(s), order(s), and related materials (collectively, "FISA materials").

The defendant, who received public notice and subsequently filed the Motion, has triggered this Court's review of the materials related to FISA-authorized[1] electronic surveillance and physical search to determine whether the FISA information was lawfully acquired and whether the electronic surveillance and physical search were made in conformity with an order of authorization or approval. Whenever "a motion is made pursuant to subsection (e) . . . to discover or obtain applications or orders or other materials relating to electronic surveillance or to discover, obtain or suppress evidence or information obtained or derived from electronic surveillance under this Act, the United States district court . . . shall . . . if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States, review in camera and ex parte the application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted." 50 U.S.C. §§ 1806(f) and 1825(g).[2] The Government is filing such an affidavit in which the Attorney General states under

---

[1] [CLASSIFIED MATERIAL REDACTED]

[2] The provisions of FISA that address electronic surveillance are found at 50 U.S.C. §§ 1801-1812; those that address physical search are found at 50 U.S.C. §§ 1821-1829. These two sets of provisions are in many respects parallel and almost identical. Citations herein are generally to

oath that disclosure or an adversary hearing would harm the national security of the United States, which is the prerequisite for the Court to review the FISA materials *in camera* and *ex parte*;[3] consequently, for the reasons below, this Court should conduct an *in camera, ex parte* review of the documents relevant to the Motion in accordance with the provisions of 50 U.S.C. §§ 1806(f) and 1825(g).[4]

The Government respectfully submits that, for the reasons set forth below, and as the Court's *in camera, ex parte* review will show: (1) the electronic surveillance and physical search at issue were both lawfully authorized and lawfully conducted in compliance with FISA; (2) disclosure to the defendant of the FISA materials and the Government's classified submissions is not authorized because the Court is able to make an accurate determination of the legality of the electronic surveillance and physical search without disclosing the FISA materials or portions thereof; (3) the FISA information should not be suppressed; (4) the FISA materials should not be disclosed; and (5) no hearing is required.

A. BACKGROUND

On December 18, 2017, Ho was charged in Indictment 17 Cr. 779 (KBF) (Indictment) with Conspiracy to Violate the Foreign Corrupt Practices Act, in violation of 18 U.S.C. § 371; four violations of the Foreign Corrupt Practices Act, in violation of 15 U.S.C. §§ 78dd-2 and/or 78dd-3, and 18 U.S.C. § 2; Conspiracy to Commit Money Laundering, in violation of 18 U.S.C. § 1956(h); and two counts of Money Laundering, in violation of 18 U.S.C. §§ 1956(a)(2)(A) and 2. (*See* Indictment, Docket Entry No. (Doc.) 24).

---

the two sets of provisions in parallel, with the first citation being to the relevant electronic surveillance provision, and the second citation being to the relevant physical search provision.

[3] The Attorney General's affidavit (Declaration and Claim of Privilege) is both filed publicly and attached as part of the Government's classified filing. *See* Sealed Exhibit 1.

[4] [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

On February 8, 2018, pursuant to 50 U.S.C. §§ 1806(c) and 1825(d), the United States provided notice to Ho and this Court that it "intends to offer into evidence, or otherwise use or disclose . . . information obtained or derived from electronic surveillance and physical search conducted pursuant to [FISA]." (*See* Doc. 45). On April 16, 2018, Ho filed the Motion. (*See* Docs. 66 and 67).

[CLASSIFIED MATERIAL REDACTED][5]

In subsequent sections of this response, the Government will: (1) present an overview of the FISA authorities at issue in this case; (2) discuss the FISA process; (3) address the manner in which the Court should conduct its *in camera, ex parte* review of the FISA materials; (4) summarize the facts supporting the FISC's probable cause determinations at issue (all of which information is contained fully in the exhibits in the Sealed Appendix); and (5) discuss the relevant minimization procedures. All of the Government's pleadings and supporting FISA materials are being submitted not only to oppose the defendant's requests, but also to support the United States' request, pursuant to FISA, that this Court: (1) conduct an *in camera, ex parte* review of the FISA materials; (2) find that the FISA information at issue was lawfully acquired and that the electronic surveillance and physical search were conducted in conformity with an order of authorization or approval; (3) find that the FISA information should be not be suppressed; and (4) order that none of the FISA materials be disclosed to the defense, and instead, that they be maintained by the United States under seal.

B. OVERVIEW OF THE FISA AUTHORITIES

[CLASSIFIED MATERIAL REDACTED]

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

1. **[CLASSIFIED MATERIAL REDACTED]**

[CLASSIFIED MATERIAL REDACTED]

2. **[CLASSIFIED MATERIAL REDACTED].**

[CLASSIFIED MATERIAL REDACTED]

3. **The FISC's Findings**

[CLASSIFIED MATERIAL REDACTED]

II. THE FISA PROCESS

A. OVERVIEW OF FISA[6]

Enacted in 1978, and subsequently amended, FISA authorizes the Chief Justice of the United States to designate eleven United States District Judges to sit as judges of the FISC. 50 U.S.C. § 1803(a)(1). The FISC judges are empowered to consider *ex parte* applications submitted by the Executive Branch for electronic surveillance and physical search when a significant purpose of the application is to obtain foreign intelligence information, as defined in FISA. Rulings of the FISC are subject to review by the Foreign Intelligence Surveillance Court of Review ("FISC of Review"), which is composed of three United States District or Circuit Judges who are designated by the Chief Justice. 50 U.S.C. § 1803(b).

As originally enacted, FISA required that a high-ranking member of the Executive Branch of Government certify that "the purpose" of the FISA application was to obtain foreign intelligence information. In 2001, FISA was amended as part of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act ("USA PATRIOT Act").[7] One change to FISA accomplished by the USA PATRIOT Act is that a high-ranking official is now required to certify that the acquisition of foreign intelligence

---

[6] This response references the statutory language in effect at the time relevant to this matter.

[7] Pub. L. No. 107-56, 115 Stat. 272 (2001).

information is "a significant purpose" of the requested electronic surveillance or physical search. 50 U.S.C. §§ 1804(a)(6)(B) and 1823(a)(6)(B).

FISA provides that the Attorney General may authorize the emergency employment of electronic surveillance and physical search if the Attorney General

> (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 title 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] 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 title to a judge having jurisdiction under section 103 as soon as practicable, but not later than seven days after the Attorney General authorizes such electronic surveillance [or physical search].

50 U.S.C. §§ 1805(e)(1) and 1824(e)(1).[8] Emergency electronic surveillance or physical search must comport with FISA's minimization requirements, which are discussed below. *See* 50 U.S.C. §§ 1805(e)(2) and 1824(e)(2).[9]

---

[8] [CLASSIFIED MATERIAL REDACTED]

[9] If no FISC order authorizing the electronic surveillance or physical search is issued, emergency surveillance or search must terminate when the information sought is obtained, when the FISC denies an application for an order, or after the expiration of seven days from the time of the emergency employment, whichever is earliest. 50 U.S.C. §§ 1805(e)(3), 1824(e)(3). Moreover, if no FISC order is issued, absent a showing of good cause, the FISC judge shall cause to be served on any United States person named in the application and on such other United States persons subject to electronic surveillance as the judge may determine in his discretion it is in the interest of justice, notice of the fact of the application, the period of the surveillance, and the fact that during the period information was or was not obtained. 50 U.S.C. §§ 1806(j), 1825(j)(1). In addition, if no FISC order is issued, neither information obtained nor evidence derived from the emergency electronic surveillance or physical search may be disclosed in any court or other proceeding, and no information concerning a United States person acquired from the electronic surveillance or physical search may be used in any other manner by Federal officers or employees without the person's consent, except with the approval of the Attorney General if the

B. THE FISA APPLICATION

FISA provides a statutory procedure whereby the Executive Branch may obtain a judicial order authorizing the use of electronic surveillance, physical search, or both, within the United States where a significant purpose is the collection of foreign intelligence information.[10] 50 U.S.C. §§ 1804(a)(6)(B) and 1823(a)(6)(B). Under FISA, "[f]oreign intelligence information" means:

> (1) information that relates to, and if concerning a United States person[11] 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 id.* § 1821(1), adopting the definitions from 50 U.S.C. § 1801. With the exception of emergency authorizations, FISA requires that a court order be obtained before any electronic surveillance or physical search may be conducted.

An application to conduct electronic surveillance pursuant to FISA must contain, among other things:

(1) the identity of the federal officer making the application;

---

information indicates a threat of death or serious bodily harm. 50 U.S.C. §§ 1805(e)(5), 1824(e)(5).

[10] [CLASSIFIED MATERIAL REDACTED]

[11] [CLASSIFIED MATERIAL REDACTED]

(2) the identity, if known, or a description of the specific target of the electronic surveillance;
(3) a statement of the facts and circumstances supporting probable cause to believe 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 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 to be followed;
(5) a detailed description of the nature of the information sought and the type of communications or activities to be subjected to the surveillance;
(6) a certification, discussed below, of a high-ranking official;
(7) a summary of the manner or means by which the electronic surveillance will be effected and a statement whether physical entry is required to effect the electronic surveillance;
(8) the facts concerning and the action taken on all previous FISA applications involving any of the persons, facilities, or places specified in the application; and
(9) the proposed duration of the electronic surveillance.

50 U.S.C. §§ 1804(a)(1)-(9).

An application to conduct a physical search pursuant to FISA must contain similar information as an application to conduct electronic surveillance except that an application to conduct a physical search must also contain a statement of the facts and circumstances that justify an 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)(1)-(8), (a)(3)(B), and (C).

1. The Certification

An application to the FISC for a FISA order must include a certification from a high-ranking executive branch official with national security responsibilities that:

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

(E) includes 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); *see also id.* § 1823(a)(6)

2. Minimization Procedures

The Attorney General has adopted, and the FISC has approved, minimization procedures that regulate the acquisition, retention, and dissemination of non-publicly available information concerning unconsenting United States persons obtained through FISA-authorized electronic surveillance or physical search, including persons who are not the targets of the FISA authorities. FISA requires that such minimization procedures be "reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information." 50 U.S.C. §§ 1801(h)(1) and 1821(4)(A).

In addition, minimization procedures also include "procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes." 50 U.S.C. §§ 1801(h)(3) and 1821(4)(c).

[CLASSIFIED MATERIAL REDACTED]

3. Attorney General's Approval

FISA further requires that the Attorney General approve applications for electronic surveillance, physical search, or both, before they are presented to the FISC.

C. THE FISC'S ORDERS

Once approved by the Attorney General, the application is submitted to the FISC and assigned to one of its judges. The FISC may approve the requested electronic surveillance, physical search, 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. § 1801(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.

50 U.S.C. §§ 1805(a)(1)-(4) and 1824(a)(1)-(4).

FISA defines "foreign power" to mean –

> (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.

50 U.S.C. §§ 1801(a)(1)-(7); *see also id.* § 1821(1) (adopting definitions from 50 U.S.C. § 1801).

"Agent of a foreign power" means –

(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);
(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 of such person's presence in the United States indicate that such person may engage in such activities in the United States, or when such person knowingly aids or abets any person in the conduct of such activities 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

(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 [the subparagraphs above] . . . or knowingly conspires with any person to engage in activities described in [the subparagraphs above.]

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

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 of the United States. 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 search, they may be considered by the FISC if there is other activity indicative that the target is an agent of a foreign power. *See United States v. Rahman*, 861 F. Supp. 247, 252 (S.D.N.Y. 1994), *aff'd*, 189 F.3d 88 (2d Cir. 1999) (wrong to conclude that statements protected by the First Amendment could not be used to conclude one is an agent of a foreign power); *United States v. Rosen*, 447 F. Supp. 2d 538, 549-50 (E.D. Va. 2006) (if probable cause to believe target, "even if engaged in First Amendment activities, may also be involved in unlawful clandestine intelligence activities" or aiding and abetting such). Additionally, FISA provides that "[i]n determining whether or not probable cause exists . . . a judge may consider past activities of the target, as well as facts and circumstances relating to current or future activities of the target." 50 U.S.C. §§ 1805(b) and 1824(b).

If the FISC has made all of the necessary findings and is satisfied that the FISA application meets the statutory provisions, the FISC issues an *ex parte* order authorizing the electronic surveillance, physical search, or both, requested in the application. 50 U.S.C. §§ 1805(a) and 1824(a). The 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 minimization procedures.

50 U.S.C. §§ 1805(c)(1) and 2(A); 1824(c)(1) and 2(A).

Under FISA, electronic surveillance or physical search targeting a United States person may be approved for up to 90 days, and those targeting a non-United States person may be approved for up to 120 days. 50 U.S.C. §§ 1805(d)(1) and 1824(d)(1). Extensions may be granted, but only if the United States submits another application that complies with FISA's requirements. An extension for electronic surveillance or physical search targeting a United States person may be approved for up to 90 days, and one targeting a non-United States person may be approved for up to one year.[12] 50 U.S.C. §§ 1805(d)(2) and 1824(d)(2).

III. THE DISTRICT COURT'S REVIEW OF FISC ORDERS

FISA authorizes the use in a criminal prosecution of information obtained or derived from any FISA-authorized electronic surveillance or physical search, provided that advance authorization is obtained from the Attorney General, 50 U.S.C. §§ 1806(b), 1825(c), and that proper notice is subsequently given to the court and to each aggrieved person against whom the information is to be used. 50 U.S.C. §§ 1806(c)-(d), 1825(d)-(e). Under Section 1806(c), the Government's notice obligation applies only if the Government (1) "intends to enter into evidence or otherwise use or disclose" (2) against an "aggrieved person" (3) in a "trial, hearing or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States" (4) any "information obtained or derived from" (5) an "electronic surveillance [or physical search] of that aggrieved person." 50 U.S.C. § 1806(c); *see* § 1825(d). Upon receiving notice, an aggrieved person against whom the information is to be used may move to suppress the use of the FISA information on two grounds: (1) the information was

[12] The FISC retains the authority to review, before the end of the authorized period of electronic surveillance or physical search, the Government's compliance with the requisite minimization procedures. 50 U.S.C. §§ 1805(d)(3) and 1824(d)(3).

unlawfully acquired; or (2) the electronic surveillance or physical search was not conducted in conformity with an order of authorization or approval. 50 U.S.C. §§ 1806(e), 1825(f). In addition, FISA contemplates that a defendant may file a motion or request under any other statute or rule of the United States to discover or obtain applications, orders, or other materials relating to electronic surveillance or physical search, *i.e.*, the FISA materials. 50 U.S.C. §§ 1806(f), 1825(g). When a defendant moves to suppress FISA information under 50 U.S.C. §§ 1806(e) or 1825(f), or seeks to discover the FISA materials under some other statute or rule, the motion or request is evaluated using FISA's probable cause standard, which is discussed below, and not the probable cause standard applicable to criminal warrants. *See, e.g.*, *United States v. El-Mezain*, 664 F.3d 467, 564 (5th Cir. 2011); *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).

A. THE REVIEW IS TO BE CONDUCTED *IN CAMERA* AND *EX PARTE*

In assessing the legality of FISA-authorized electronic surveillance and physical search, or both, the district court

> shall, notwithstanding any other law, if the Attorney General files an affidavit or declaration under oath that disclosure or an adversary hearing would harm the national security of the United States, review in camera and ex parte the application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted.[13]

50 U.S.C. §§ 1806(f) and 1825(g). On the filing of the Attorney General's affidavit or declaration (which accompanies this response), 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

[13] [CLASSIFIED MATERIAL REDACTED]

necessary to make an accurate determination of the legality of the surveillance [or search]."[14] 50 U.S.C. §§ 1806(f) and 1825(g). Thus, the propriety of the disclosure of any FISA applications or orders to a defendant may not even be considered unless and until the district court has first concluded that it is unable to make an accurate determination of the legality of the acquired collection after reviewing the Government's submissions (and any supplemental pleadings that the district court may request) *in camera* and *ex parte*. *See United States v. Abu-Jihaad*, 630 F.3d 102, 129 (2d Cir. 2010) (disclosure of FISA materials "is the exception and *ex parte, in camera* determination is the rule" (quoting *United States v. Stewart*, 590 F.3d 93, 129 (2d Cir. 2009)); *United States v. Huang*, 15 F. Supp. 3d 1131, 1138 (D.N.M. Apr. 22, 2014) ("Disclosure may be ordered only if the district court cannot make an accurate determination of the legality of the surveillance or search."); *United States v. Omar*, 786 F.3d 1104, 1110 (8th Cir. 2015) ("[D]isclosure and an adversary hearing are the exception occurring *only* when necessary." (quoting *United States v. Isa*, 923 F.2d 1300, 1306 (8th Cir. 1991), which in turn quoted *United States v. Belfield*, 692 F.2d 141, 147 (D.C. Cir. 1982))) (emphasis in original); *El-Mezain*, 664 F.3d at 565 (quoting 50 U.S.C. § 1806(f) and emphasizing the word "necessary").

1. *In Camera, Ex Parte* Review Is the Rule

Federal courts, including those in the Second Circuit, have repeatedly and consistently held that FISA anticipates an "*ex parte*, *in camera* determination is to be the rule," *Duggan*, 743 F.2d at 78 (quoting *Belfield*, 692 F.2d at 147), with disclosure and an adversarial hearing being

[14] In *United States v. Duggan*, the Second Circuit explained that disclosure might be necessary "if the judge's initial review revealed potential irregularities such as 'possible misrepresentations of fact, vague identification of 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.'" 743 F.2d 59, 78 (2d Cir. 1984) (quoting S. Rep. 95-604, at 58 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3904, 3960).

the "exception, occurring *only* when necessary."[15] *Omar*, 786 F.3d at 1110 (citing *Isa*, 923 F.2d at 1306). In fact, every court but one (whose decision was subsequently overturned by an appellate court)[16] that has addressed a motion to disclose FISA materials or to suppress FISA information has been able to reach a conclusion as to the legality of the FISA collection at issue based on its *in camera, ex parte* review. *See Stewart*, 590 F.3d at 128 ("'[*E*]*x parte, in camera* determination is to be the rule'" (quoting *Belfield*, 692 F.2d at 147)); *El-Mezain*, 664 F.3d at 566-67 (quoting district court's statement that no court has ever held an adversarial hearing to assist the court); *In re Grand Jury Proceedings of the Special Apr. 2002 Grand Jury* ("*In re Grand Jury Proceedings*"), 347 F.3d 197, 203 (7th Cir. 2003) (noting that no court had ever ordered disclosure of FISA materials); *United States v. Medunjanin*, No. 10 Cr. 191 (RJD), 2012 WL 526428, at *10 (E.D.N.Y. Feb. 16, 2012) (noting that "[n]o United States District Court or Court of Appeals has ever determined that disclosure to the defense of such materials was necessary to determine the lawfulness of surveillance or searches under FISA" (quoting *United States v. Warsame*, 547 F. Supp. 2d 982, 987 (D. Minn. 2008))); *Abu-Jihaad*, 531 F. Supp. 2d at 310 ("Courts have uniformly held that *ex parte* and *in camera* inspections are the 'rule' under FISA. . . ." (citing *Duggan*, 743 F. 2d at 78)); *United States v. Thomson,* 752 F. Supp. 75, 77 (W.D.N.Y.

---

[15] The defendant is requesting *in camera, ex parte* review by this Court. (*See* Def. Mem. 3-4). The defense makes no specific arguments regarding why disclosure of the FISA materials and suppression of the FISA information is necessary in this case. The defendant reserves the right to move for disclosure under 50 U.S.C. §§ 1806(g), 1825(h). The Government reserves the right to respond to such an argument, if made by the defense.

[16] In *United States v. Daoud*, the district court ruled that it was capable of making the determination, but nevertheless ordered the disclosure of FISA materials to the defense. No. 12 Cr 723, 2014 WL 321384, at *8 (N.D. Ill. Jan. 29, 2014). The Government appealed the *Daoud* court's order to the U.S. Court of Appeals for the Seventh Circuit, which overturned the district court's decision to disclose FISA materials, stating, "[s]o clear is it that the materials were properly withheld from defense counsel that there is no need for a remand to enable the district judge to come to the same conclusion, because she would have to do so." *United States v. Daoud*, 755 F.3d 479, 485 (7th Cir. 2014).

1990) (noting that no court "has found disclosure or an adversary hearing necessary"); *United States v. Sattar*, No. 02 Cr. 395 (JGK), 2003 WL 22137012, at *6 (S.D.N.Y. Sept. 15, 2003) (noting "this court knows of no instance in which a court has required an adversary hearing or disclosure in determining the legality of a FISA surveillance" (citing *United States v. Nicholson*, 955 F. Supp. 588, 592 & n.11 (E.D. Va. 1997)).

As the exhibits in the Sealed Appendix make clear, there is nothing extraordinary about the FISA-authorized electronic surveillance and physical search in this case that would justify the production and disclosure of highly sensitive and classified FISA materials or the suppression of FISA-obtained or -derived evidence. Here, the FISA materials are well-organized and easily reviewable by the Court *in camera* and *ex parte*, and they are fully and facially sufficient to allow the Court to make an accurate determination that the FISA information was lawfully acquired and that the electronic surveillance and physical search were made in conformity with an order of authorization or approval. In other words, the materials presented "are straightforward and readily understood." *In re Kevork*, 634 F. Supp. 1002, 1008 (C.D. Cal. 1985), *aff'd*, 788 F.2d 566 (9th Cir. 1986). Moreover, as in other cases, "[t]he determination of legality in this case is not complex." *Belfield*, 692 F.2d at 147; *see also United States v. Hasbajrami*, No. 11 Cr. 623 (JG), 2016 WL 1029500, at *14 (E.D.N.Y. Feb. 18, 2016) (finding the review of the FISA materials was "relatively straightforward and not complex" such that the court "was able to evaluate the legality of the challenged surveillance without concluding that due process first warranted disclosure") (internal quotation marks and citations omitted); *Warsame*, 547 F. Supp. 2d at 987 (finding that the "issues presented by the FISA applications are straightforward and uncontroversial"); *Abu-Jihaad*, 531 F. Supp. 2d at 310; *Thomson*, 752 F. Supp. at 79. This Court, much like the aforementioned courts, is fully capable of reviewing the

FISA materials *in camera* and *ex parte* and making the requisite legal determination without an adversarial hearing.

In addition to the specific harm that would result from the disclosure of the FISA materials in this case, which is detailed in the classified declaration of an Assistant Director of the FBI in support of the Attorney General's Declaration and Claim of Privilege, the underlying rationale for non-disclosure is clear: "In the sensitive area of foreign intelligence gathering, the need for extreme caution and sometimes even secrecy may not be overemphasized." *United States v. Ott*, 637 F. Supp. 62, 65 (E.D. Cal. 1986), *aff'd*, 827 F.2d 473 (9th Cir. 1987); *accord Isa*, 923 F.2d at 1306 (the Court's "study of the materials leaves no doubt that substantial national security interests required the *in camera, ex parte* review, and that the district court properly conducted such a review"); *Medunjanin*, 2012 WL 526428, at *9 (finding persuasive the Government's argument that "unsealing the FISA materials in this case would provide the defense with unnecessary details of an extraordinarily sensitive anti-terrorism investigation").

Confidentiality is critical to national security. "If potentially valuable intelligence sources" believe that the United States "will be unable to maintain the confidentiality of its relationship to them, many [of those sources] could well refuse to supply information. . . ." *Central Intelligence Agency v. Sims*, 471 U.S. 159, 175 (1985). When considering whether the disclosure of classified sources, methods, techniques, or information would harm the national security, federal courts have expressed a great reluctance to replace the considered judgment of Executive Branch officials charged with the responsibility of weighing a variety of subtle and complex factors in determining whether the disclosure of information may lead to an unacceptable risk of compromising the intelligence gathering process, and determining whether foreign agents, spies, and terrorists are capable of piecing together a mosaic of information that,

if revealed, could reasonably be expected to harm the national security of the United States. *See Sims*, 471 U.S. at 180; *United States v. Yunis*, 867 F.2d 617, 623 (D.C. Cir. 1989) ("Things that did not make sense to the District Judge would make all too much sense to a foreign counter-intelligence specialist who could learn much about this nation's intelligence-gathering capabilities from what these documents revealed about sources and methods."); *Halperin v. Central Intelligence Agency*, 629 F.2d 144, 150 (D.C. Cir. 1980) (noting that "each individual piece of intelligence information, much like a piece of jigsaw puzzle, may aid in piecing together other bits of information even when the individual piece is not of obvious importance in itself"); *Medunjanin*, 2012 WL 526428, at *10 (quoting *Yunis*, 867 F.2d at 625). An adversary hearing is not only unnecessary to aid the Court in the straightforward task before it, but such a hearing would also create potential dangers that courts have consistently sought to avoid.

As the Second Circuit explained in *Stewart*:

> FISA applications are likely to contain allegedly sensitive information relating to perceived issues of national security. The applications are required to set forth how and why the Executive Branch knows what it knows, which may include references to covert agents and informers. For this reason, *ex parte*, *in camera* determination is to be the rule.

590 F.3d at 128 (quoting *Duggan*, 743 F.2d at 77).

2. *In Camera, Ex Parte* Review Is Constitutional

The constitutionality of FISA's *in camera*, *ex parte* review provisions has been affirmed by every federal court that has considered the matter, including the Second Circuit and the Southern District of New York. *See Abu-Jihaad*, 630 F.3d at 129 (affirming district court's determination that "its *in camera*, *ex parte* review permitted it to assess the legality of the challenged surveillance and the requirements of due process did not counsel otherwise"); *Stewart*, 590 F.3d at 126 (noting that "the procedures fashioned in FISA [are] a constitutionally adequate balancing of the individual's Fourth Amendment rights against the nation's need to

obtain foreign intelligence information." (quoting *Duggan*, 743 F. 2d at 73)); *United States v. Fishenko*, No. 12 Civ. 626 (SJ), 2014 WL 8404215, at *7 (E.D.N.Y. Sept. 25, 2014) (citing numerous decisions by U.S. district courts in the Second Circuit and concluding that "there is no question as to the constitutionality of FISA"); *Sattar*, 2003 WL 22137012, at *5-6; *accord Duka*, 671 F.3d at 337 (rejecting the defendant's constitutional challenge to the use of FISA-derived evidence at trial, thereby "[a]ligning with all of the other courts of appeals that have considered this issue"); *El-Mezain*, 664 F.3d at 567 (agreeing with district court that its *in camera, ex parte* review ensured the defendant's constitutional and statutory rights were not violated); *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"); *ACLU Found. of S. Cal. v. Barr*, 952 F.2d 457, 465 (D.C. Cir. 1991) (procedure under FISA "is an acceptable means of adjudicating the constitutional rights of persons who have been subjected to FISA surveillance" (citing *Belfield*, 692 F.2d at 141)); *Ott*, 827 F.2d at 476-77 (FISA's review procedures do not deprive a defendant of due process).

In summary, FISA mandates a process by which the district court must conduct an initial *in camera, ex parte* review of FISA applications, orders, and related materials to determine whether the FISA information was lawfully acquired and whether the electronic surveillance and physical search were made in conformity with an order of authorization or approval. *In camera, ex parte* review is the rule in such cases, and that procedure is constitutional. In this case, the Attorney General has filed the required declaration invoking that procedure and has declared that disclosure or an adversary hearing would harm national security. Accordingly, an *in camera, ex parte* review by this Court is the appropriate method to determine whether the FISA information

was lawfully acquired and whether the electronic surveillance and physical search were conducted in conformity with an order of authorization or approval.

B. THE DISTRICT COURT'S SUBSTANTIVE REVIEW

1. Standard of Review of Probable Cause

In evaluating the legality of the FISA collection, a district court's review should determine: (1) whether the certification submitted by the Executive Branch in support of a FISA application was properly made; (2) whether the application established the probable cause showing required by FISA; and (3) whether the collection was properly minimized. *See Abu-Jihaad*, 630 F.3d at 130-31; *see also* 50 U.S.C. §§ 1806(a), (f), 1824(a), 1825(g).

Although federal courts are not in agreement as to whether the FISC's probable cause determination should be reviewed *de novo* or afforded due deference, courts in the Second Circuit afford due deference to the determinations of the FISC.[17] *See Abu-Jihaad*, 630 F.3d at 130; *Stewart*, 590 F.3d at 128; *Hasbajrami*, 2016 WL 1029500, at *13; *Fishenko*, 2014 WL 8404215, at *8; *cf. Medunjanin*, 2012 WL 526428, at *6-7 (affording deferential review, but noting that such review is not superficial).

2. Probable Cause Standard

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 is directed is being used, or is about to be used, or that the property or premises to be searched is, or is about

[17] Federal courts in other circuits have determined that the probable cause determination of the FISC should be reviewed *de novo*. *See United States v. Hammoud*, 381 F.3d 316, 332 (4th Cir. 2004), *rev'd on other grounds*, 543 U.S. 1097 (2005), *op. reinstated in pertinent part*, 405 F.3d 1034 (4th Cir. 2005); *Rosen*, 447 F. Supp. 2d at 545; *Warsame*, 547 F. Supp. 2d at 990-91; *United States v. Kashmiri*, No. 09 Cr. 830-4, 2010 WL 4705159, at *1 (N.D. Ill. Nov. 10, 2010); *United States v. Nicholson*, No. 09 C. 40 (BR), 2010 WL 1641167, at *5 (D. Or. Apr. 20, 2010). In each of these cases, the courts applied a *de novo* standard in reviewing the FISC's probable cause findings, and each court found that applications before it contained probable cause.

to be, owned, used, possessed by, or is in transit to or from, a foreign power or an agent of a foreign power. 50 U.S.C. §§ 1805(a), 1824(a); *Abu-Jihaad*, 630 F.3d at 130. It is this standard – not the standard applicable to criminal search warrants – that this Court must apply. *Medunjanin*, 2012 WL 526428, at *6 ("[N]o branch of government – whether executive or judicial – need make a probable cause finding of *actual or potential* criminal activity to justify a FISA warrant"); *El-Mezain*, 664 F.3d at 564; *United States v. Cavanagh*, 807 F.2d 787, 790 (9th Cir. 1987) (citing *United States v. United States District Court (Keith)*, 407 U.S. 297, 322 (1972)).

The probable cause showing the Government must satisfy before receiving authorization to conduct electronic surveillance or physical search under FISA complies with the Fourth Amendment's reasonableness standard. The argument that FISA's different probable cause standard violates the Fourth Amendment's reasonableness requirement has been uniformly rejected by federal courts. *See, e.g.*, *Abu-Jihaad*, 630 F.3d at 120 (rejecting the defendant's Fourth Amendment claim and listing 16 cases that stand for the proposition that FISA does not violate the Fourth Amendment).

[CLASSIFIED MATERIAL REDACTED]

3. Standard of Review of Certifications

Certifications submitted in support of a FISA application should be "subjected to only minimal scrutiny by the courts," and are "presumed valid." *Duggan*, 743 F.2d at 77 & n.6 (citing *Franks v. Delaware*, 438 U.S. 154, 171 (1978)); *United States v. Campa*, 529 F.3d 980, 993 (11th Cir. 2008) (quoting *United States v. Badia*, 827 F.2d 1458, 1463 (11th Cir. 1987)); *United States v. Sherifi*, 793 F. Supp. 2d 751, 760 (E.D.N.C. 2011); *Warsame*, 547 F. Supp. 2d at 990. 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. A district court's review should determine whether the certifications were made in accordance with FISA's requirements. Congress intended that the reviewing district court should "have no greater authority to second-guess the executive branch's certifications than has the FISA judge." *Id.*; *Rahman*, 861 F. Supp. at 250 (citing *Duggan*); *United States v. Omar*, No. CR-09-242, 2012 WL 2357734, at *3 (D. Minn. June 20, 2012) ("The reviewing court must presume as valid 'the representations and certifications submitted in support of an application for FISA surveillance' . . . absent a showing sufficient to trigger a *Franks* hearing." (quoting *Duggan*, 743 F. 2d at 77)); *In re Grand Jury Proceedings*, 347 F.3d at 204-05; *Badia*, 827 F.2d at 1463; *Kashmiri*, 2010 WL 4705159, at *1; *United States v. Islamic Am. Relief Agency* (*IARA*), No. 07-87-Cr-NKL, 2009 WL 5169536, at *4 (W.D. Mo. Dec. 21, 2009). When the target is a United States person, the district court should also ensure that each certification is not "clearly erroneous." *Duggan*, 743 F.2d at 77; *Campa*, 529 F.3d at 994; *Kashmiri*, 2010 WL 4705159, at *2. A "clearly erroneous" finding is established only when "the reviewing court on the [basis of the] entire evidence 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); *United States v. Garcia*, 413 F.3d 201, 222 (2d Cir. 2005) (quoting *U.S. Gypsum Co.*, 333 U.S. at 395).

4. <u>FISA Is Subject to the "Good Faith" Exception</u>

Even assuming *arguendo* that this Court determines that a particular FISC order was not supported by probable cause, or that one or more of the FISA certification requirements were not met (and there is no basis for either determination in this case), the evidence obtained or derived from the FISA-authorized electronic surveillance and physical search is, nonetheless,

admissible under the "good faith" exception to the exclusionary rule articulated in *United States v. Leon*, 468 U.S. 897 (1984). *See United States v. Ahmed*, No. 06 Cr. 147 (WSD) (GGB), 2009 U.S. Dist. LEXIS 120007, at *25 n.8, 26-27 (N.D. Ga. Mar 19, 2009) (noting that federal officers are entitled to rely in good faith on a FISA warrant) (citing *United States v. Ning Wen*, 477 F.3d 896, 897 (7th Cir. 2007)).

The FISA-authorized electronic surveillance and physical search at issue in this case, authorized by a duly enacted statute and an order issued by a neutral judicial officer, would fall squarely within this good faith exception (were the Court to reach the question, which it need not). There is no basis to find that any declarations or certifications at issue in this case were deliberately or recklessly false. *See Leon*, 468 U.S. at 914-15; *Massachusetts v. Sheppard*, 468 U.S. 981, 987-88 (1984). Further, there are no facts indicating that the FISC failed to act in a neutral and detached manner in authorizing the electronic surveillance and physical search at issue. *See Leon*, 468 U.S. at 914-15. Moreover, as the Court will see from its *in camera, ex parte* review of the FISA materials, facts establishing the requisite probable cause were submitted to the FISC, the FISC's orders contained all of the requisite findings, and "well-trained officers" reasonably relied on those orders. Therefore, in the event that the Court questions whether a particular FISC order was supported by sufficient probable cause, the information obtained pursuant to that order would be admissible under *Leon*'s "good faith" exception to the exclusionary rule.

IV. THE FISA INFORMATION WAS LAWFULLY ACQUIRED AND THE ELECTRONIC SURVEILLANCE AND PHYSICAL SEARCH WERE MADE IN CONFORMITY WITH AN ORDER OF AUTHORIZATION OR APPROVAL

[CLASSIFIED MATERIAL REDACTED]

A. THE INSTANT FISA APPLICATION(S) MET FISA'S PROBABLE CAUSE STANDARD

[CLASSIFIED MATERIAL REDACTED]

1. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

2. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

a. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

b. [CLASSIFIED MATERIAL REDACTED].

[CLASSIFIED MATERIAL REDACTED]

c. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

d. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

e. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

f. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

g. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

3. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

a. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED].

i. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

ii. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED][18]

b. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

i. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

c. Conclusion: There Was Sufficient Probable Cause to Establish that the Information Acquired from the Targeted Facilities, Places, Property, or Premises Was Lawfully Acquired

[CLASSIFIED MATERIAL REDACTED]

B. THE CERTIFICATIONS COMPLIED WITH FISA

[CLASSIFIED MATERIAL REDACTED]

1. Foreign Intelligence Information

[CLASSIFIED MATERIAL REDACTED]

2. "A Significant Purpose"

[CLASSIFIED MATERIAL REDACTED]

---

[18] CLEAR is a public records database designed for Government and law enforcement, which uses public and proprietary records, including cellular telephone and utility company data, as well as information from social networking websites, blogs, and news websites to compile information.

3. Information Not Reasonably Obtainable Through Normal Investigative Techniques

[CLASSIFIED MATERIAL REDACTED]

C. THE ELECTRONIC SURVEILLANCE AND PHYSICAL SEARCH WERE CONDUCTED IN CONFORMITY WITH AN ORDER OF AUTHORIZATION OR APPROVAL

This Court's *in camera, ex parte* review of the FISA materials will demonstrate that the electronic surveillance and physical search were conducted in conformity with an order of authorization or approval (*i.e.*, lawfully conducted). That is, the FISA-obtained or -derived information in this case was acquired, retained, and disseminated by the FBI in accordance with FISA's minimization requirements, the standard minimization procedures ("SMPs") adopted by the Attorney General and approved by the FISC.

1. The Standard Minimization Procedures

Once a reviewing court is satisfied that the electronic surveillance and physical search were properly certified and the information was lawfully acquired pursuant to FISA, it must then examine whether the electronic surveillance and physical search were lawfully conducted. *See* 50 U.S.C. §§ 1806(e)(2) and 1825(f)(1)(B). In order to examine whether the electronic surveillance and physical search were lawfully conducted, the reviewing court must determine whether the Government followed the relevant minimization procedures to appropriately minimize the information acquired pursuant to FISA.

[CLASSIFIED MATERIAL REDACTED]

FISA's legislative history and the applicable case law demonstrate that the definitions of "minimization procedures" and "foreign intelligence information" were intended to take into account the realities of collecting foreign intelligence because the activities of persons engaged in clandestine intelligence gathering or international terrorism are often not obvious on their face.

See Rahman, 861 F. Supp. at 252-53. The degree to which information is required to be minimized varies somewhat given the specifics of a particular investigation, such that less minimization at acquisition is justified when "the investigation is focusing on what is thought to be a widespread conspiracy" and more extensive surveillance is necessary "to determine the precise scope of the enterprise." *In re Sealed Case*, 310 F.3d at 717, 741 (FISC Ct. Rev. 2002); *see also United States v. Bin Laden*, 126 F. Supp. 2d 264, 286 (S.D.N.Y. 2000) ("More extensive monitoring and greater leeway in minimization efforts are permitted in a case like this given the world-wide, covert and diffuse nature of the international terrorist group(s) targeted." (internal quotation marks omitted)). Furthermore, the activities of foreign powers and their agents are often not obvious from an initial or cursory overhear of conversations. To the contrary, agents of foreign powers frequently engage in coded communications, compartmentalized operations, the use of false identities and other practices designed to conceal the breadth and aim of their operations, organization, activities, and plans. *See, e.g.*, *United States v. Salameh*, 152 F.3d 88, 154 (2d Cir. 1998) (noting that two conspirators involved in the 1993 bombing of the World Trade Center in New York referred to the bomb plot as the "study" and to terrorist materials as "university papers"). As one court explained, "[i]nnocuous-sounding conversations may in fact be signals of important activity; information on its face innocent when analyzed or considered with other information may become critical." *Kevork*, 634 F. Supp. at 1017 (quoting H.R. Rep. No. 95-1283, 95th Cong., 2d Sess., Pt. 1, at 55 (1978) (hereinafter "House Report")); *see also Hammoud*, 381 F.3d at 334, *rev'd on other grounds*, 543 U.S. 1097 (2005), *op. reinstated in pertinent part*, 405 F.3d 1034 (4th Cir. 2005) (citing *Salameh*, 152 F.3d at 154); *In re Sealed Case*, 310 F.3d at 740-41 (intercepted communications may be in code or foreign language with no readily available translator); *Thomson*, 752 F. Supp. at 81 (noting that it is permissible to

retain and disseminate "bits and pieces" of information until the information's "full significance becomes apparent") (citing House Report, part 1, at 58); *Bin Laden*, 126 F. Supp. 2d at 286 (facts can support automated recording of phones). Likewise, "individual items of information, not apparently significant when taken in isolation, may become highly significant when considered together over time." *Rahman*, 861 F. Supp. at 252-53 (citing House Report, part 1, at 55, 59). The Government must be given flexibility where the conversations are carried out in a foreign language. *United States v. Mubayyid*, 521 F. Supp. 2d 125, 134 (D. Mass. 2007); *Rahman*, 861 F. Supp. at 252. As a result, "courts have construed 'foreign intelligence information' broadly and sensibly allowed the government some latitude in its determination of what is foreign intelligence information." *Rosen*, 447 F. Supp. 2d at 551.

The nature of the foreign intelligence information sought also impacts implementation of the minimization procedures at the retention and dissemination stages. There is a legitimate need to conduct a thorough post-acquisition review of FISA information that involves a United States person who is acting as an agent of a foreign power. As Congress explained:

> It is "necessary" to identify anyone working with him in this network, feeding him information, or to whom he reports. Therefore, it is necessary to acquire, retain and disseminate information concerning all his contacts and acquaintances and his movements. Among his contacts and acquaintances, however, there are likely to be a large number of innocent persons. Yet, information concerning these persons must be retained at least until it is determined that they are not involved in the clandestine intelligence activities and may have to be disseminated in order to determine their innocence.

House Report, part 1, at 58. Indeed, at least one court has cautioned that, when a U.S. person communicates with an agent of a foreign power, the Government would be "remiss in meeting its foreign counterintelligence responsibilities" if it did not thoroughly "investigate such contacts and gather information to determine the nature of those activities." *Thomson*, 752 F. Supp. at 82.

Congress also recognized that agents of a foreign power are often very sophisticated and skilled at hiding their activities. *Cf. id.* at 81 (quoting House Report part 1, at 58). Accordingly,

to pursue leads, Congress intended that the Government be given "a significant degree of latitude" with respect to the "retention of information and the dissemination of information between and among counterintelligence components of the Government." *Cf. id.*

In light of these realities, Congress recognized that "no electronic surveillance can be so conducted that innocent conversations can be totally eliminated." *See* S. Rep. No. 95-701, 95th Cong., 2d Sess., 39 (quoting *Keith*, 407 U.S. at 323) (1978) ("Senate Report"). The Fourth Circuit reached the same conclusion in *Hammoud*, stating that the "mere fact that innocent conversations were recorded, without more, does not establish that the government failed to appropriately minimize surveillance." 381 F.3d at 334.

Accordingly, in reviewing the adequacy of minimization efforts, the test to be applied is neither whether innocent conversations were intercepted, nor whether mistakes were made with respect to particular communications. Rather, as the Supreme Court stated in the context of Title III surveillance, there should be 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). "The test of compliance is 'whether a good-faith effort to minimize was made.'" *Mubayyid*, 521 F. Supp. 2d at 135; *see also Hammoud*, 381 F.3d at 334 ("The minimization requirement obligates the government to make a good faith effort to minimize the acquisition and retention of irrelevant information."); Senate Report at 39-40 (stating that 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"); *IARA*, 2009 WL 5169536, at *6 (quoting Senate Report at 39-40).

Moreover, as noted above, FISA expressly states that 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) and 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. *See id.* at 1305.

Even in the limited occasions described herein, when certain communications were not properly minimized, suppression would not be the appropriate remedy with respect to those communications that met the standard. *Cf. United States v. Falcone*, 364 F. Supp. 877, 886-87 (D.N.J. 1973), *aff'd*, 500 F.2d 1401 (3d Cir. 1974) (reaching a similar conclusion in the context of Title III). As discussed above, absent evidence that "on the whole" there has been a "complete" disregard for the minimization procedures, the fact that some communications should have been minimized does not affect the admissibility of others that were properly acquired and retained. Indeed, Congress specifically intended that the only evidence that should be suppressed is the "evidence which was obtained unlawfully." House Report at 93. FISA's legislative history reflects that Congress intended only a limited sanction for errors of minimization:

> As the language of the bill makes clear, only that evidence which was obtained unlawfully or derived from information obtained unlawfully would be suppressed. If, for example, some information should have been minimized but was not, only that information should be suppressed; the other information obtained lawfully should not be suppressed.

Id.; *see also Falcone*, 364 F. Supp. at 886-87; *accord United States v. Medunjanin*, No. 10 Cr. 19-1, 2012 WL 526428, at *12 (E.D.N.Y. Feb. 16, 2012) (disclosure and suppression not warranted where "failure to adhere to [the minimization] protocol was *de minimis*").

2. The FISA Information Was Appropriately Minimized

[CLASSIFIED MATERIAL REDACTED]

Based upon this information, the Government lawfully conducted the FISA collections discussed. Consequently, for the reasons stated above, the Court should find that the FISA collections discussed were lawfully conducted under the minimization procedures approved by the FISC.

V. CONCLUSION: THERE IS NO BASIS FOR THE COURT TO DISCLOSE THE FISA MATERIALS OR TO SUPPRESS THE FISA INFORMATION

For the foregoing reasons, the defendant's motion should be denied without a hearing. The Attorney General has filed a declaration in this case stating that disclosure of or an adversary hearing with respect to the FISA materials would harm the national security of the United States. Therefore, FISA mandates that this Court conduct an *in camera, ex parte* review of the challenged FISA materials to determine whether the information was lawfully acquired and whether the electronic surveillance and physical search were made in conformity with an order of authorization or approval. In conducting that review, the Court may disclose the FISA materials "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). Congress, in enacting FISA's procedures for *in camera, ex parte* judicial review, has balanced and accommodated the competing interests of the Government and criminal defendants, and has articulated the standard for disclosure; that is, only where the Court finds that disclosure is necessary to the Court's accurate determination of the legality of the FISA collection.

The Government respectfully submits that the Court can make this determination without disclosing the classified and highly sensitive FISA materials to the defendant. The FISA materials at issue here, which have been submitted for *in camera, ex parte* review in the Sealed

Appendix, are organized and readily understood, and an overview of them has been presented herein as a frame of reference. This Court will be able to render a determination based on its *in camera, ex parte* review, and the defendant makes no argument for supplanting Congress' reasoned judgment with a different proposed standard of review.

Furthermore, the Government respectfully submits that the Court's examination of the FISA materials in the Sealed Appendix will demonstrate that the Government satisfied FISA's requirements to obtain orders for electronic surveillance and physical search, that the information obtained pursuant to FISA was lawfully acquired, and that the electronic surveillance and physical search were made in conformity with an order of authorization or approval.

Even if this Court were to determine that the FISA information was not lawfully acquired or that the electronic surveillance and physical search were not made in conformity with an order of authorization or approval, the FISA evidence would nevertheless be admissible under the good faith exception to the exclusionary rule articulated in *Leon*, 468 U.S. 897. *See also Ning Wen*, 477 F.3d at 897 (the *Leon* good faith exception applies to FISA orders); *Ahmed*, 2009 U.S. Dist. LEXIS 120007, at *25 n.8.

Based on the foregoing analysis, the Government respectfully submits that the Court must conduct an *in camera, ex parte* review of the FISA materials and the Government's classified submission, and should: (1) find that the electronic surveillance and physical search at issue in this case were both lawfully authorized and lawfully conducted; (2) hold that disclosure of the FISA materials and the Government's classified submissions to the defendant is not authorized because the Court is able to make an accurate determination of the legality of the surveillance and search without disclosing the FISA materials or any portions thereof; (3) hold that the fruits of electronic surveillance and physical search should not be suppressed; (4) deny

the defendant's motion without an evidentiary hearing; and (5) order that the FISA materials and the Government's classified submissions be maintained under seal by the Classified Information Security Officer or his or her designee.[19]

DATED: New York, New York
July 12, 2018

Respectfully submitted,

GEOFFREY S. BERMAN
United States Attorney

By: s/ Daniel C. Richenthal
Daniel C. Richenthal
Andrew DeFilippis
Assistant United States Attorneys
(212) 637-2109/2267

By: s/ Kim A. Robbins-Segers
Kim A. Robbins-Segers
Attorney
United States Department of Justice
National Security Division
Washington, DC 20530
(202) 305-0867

By: s/ Patrick Murphy
Patrick Murphy
Trial Attorney
United States Department of Justice
National Security Division
Washington, DC 20530
(202) 233-2093

[19] A district court order granting motions or requests under 50 U.S.C. §§ 1806(g) or 1825(h), a decision that electronic surveillance and physical search were not lawfully authorized or conducted, and an order requiring the disclosure of FISA materials is each a final order for purposes of appeal. 50 U.S.C. §§ 1806(h), 1825(i). Should the Court conclude that disclosure of any item within any of the FISA materials or suppression of any FISA-obtained or -derived information may be required, given the significant national security consequences that would result from such disclosure or suppression, the Government would expect to pursue an appeal. Accordingly, the Government respectfully requests that the Court indicate its intent to do so before issuing any order, and that the Court stay any such order pending an appeal by the United States of that order.