STEPHANIE YONEKURA
Acting United States Attorney
ROBERT E. DUGDALE
Assistant United States Attorney
Chief, Criminal Division
ANTHONY J. LEWIS (Cal. Bar No. 231825)
Assistant United States Attorney
National Security Section
1300 United States Courthouse
312 North Spring Street
Los Angeles, California 90012
Telephone: (213) 894-1786
Facsimile: (213) 894-6436
E-mail: anthony.lewis@usdoj.gov
CASEY ARROWOOD
Trial Attorney
Counterespionage Section
National Security Division

Attorneys for Plaintiff
UNITED STATES OF AMERICA

UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA, Plaintiff, v. KEITH PRESTON GARTENLAUB, Defendant.	No. SA CR 14-173-CAS <u>GOVERNMENT'S UNCLASSIFIED MEMORANDUM IN OPPOSITION TO DEFENDANT'S MOTION FOR DISCLOSURE OF FISA MATERIAL AND MEMORANDUM OF POINT AND AUTHORITIES TO SUPPRESS THE FRUITS OR DERIVATIVES OF ANY EVIDENCE COLLECTED PURSUANT TO FISA OR ANY OTHER FOREIGN INTELLIGENCE GATHERING</u>

Plaintiff United States of America, by and through its counsel of record, the United States Attorney for the Central District of California and Assistant United States Attorney Anthony Lewis, hereby files the Government's Unclassified Memorandum in Opposition to Defendant's Motion for Disclosure of FISA Material and Memorandum of Point and Authorities to Suppress the Fruits or Derivatives of Any Evidence Collected Pursuant to FISA or Other Foreign Intelligence Gathering.

This memorandum in opposition is based upon the attached memorandum of points and authorities, the files and records in this case, and such further evidence and argument as the Court may permit.

Dated: May 4, 2015

Respectfully submitted,

STEPHANIE YONEKURA
Acting United States Attorney

ROBERT E. DUGDALE
Assistant United States Attorney
Chief, Criminal Division

/s/
ANTHONY LEWIS
Assistant United States Attorney

CASEY ARROWOOD
Trial Attorney

Attorneys for Plaintiff
UNITED STATES OF AMERICA

TABLE OF CONTENTS

DESCRIPTION PAGE

TABLE OF CONTENTS

TABLE OF CONTENTS

DESCRIPTION PAGE

TABLE OF AUTHORITIES

DESCRIPTION **PAGE**

FEDERAL CASES

TABLE OF AUTHORITIES

DESCRIPTION PAGE

FEDERAL CASES CONT'D

TABLE OF AUTHORITIES

DESCRIPTION PAGE

FEDERAL CASES CONT'D

TABLE OF AUTHORITIES

DESCRIPTION PAGE

FEDERAL CASES CONT'D

TABLE OF AUTHORITIES

DESCRIPTION PAGE

FEDERAL CASES CONT'D

TABLE OF AUTHORITIES

DESCRIPTION PAGE

FEDERAL CASES CONT'D

TABLE OF AUTHORITIES

I. INTRODUCTION

The Government is filing this unclassified memorandum in opposition to defendant Keith Preston Gartenlaub's (Gartenlaub) Motion for Disclosure and Memorandum of Point and Authorities to Suppress the Fruits or Derivatives of Any Evidence Collected Pursuant to FISA or Other Foreign Intelligence Gathering (defendant's motion) (Docket Entry (Doc.) 70). The defendant seeks: (1) disclosure of the documents underlying electronic surveillance and physical searches conducted pursuant to the Foreign Intelligence Surveillance Act (FISA) (i.e., the FISA materials); and (2) suppression of any evidence derived from FISA search or surveillance (i.e., the FISA information). Doc. 70 at pp. 2-3.[1]

[CLASSIFIED MATERIAL REDACTED][2,3]

For the reasons set forth below and from the Court's in camera, ex parte review of the FISA materials submitted herewith, it is conclusively established that: (1) the electronic surveillance and physical searches at issue were both lawfully authorized and lawfully

---

[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 searches 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 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 filed both publicly and as an exhibit in the Sealed Appendix to this unclassified filing. See Sealed Exhibit 1.

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 surveillance and searches without disclosing the FISA materials or portions thereof; (3) the fruits of the electronic surveillance and physical searches should not be suppressed; (4) the defendant's motion should be denied to the extent that it seeks disclosure of FISA materials; and (5) no hearing is required.

A. BACKGROUND

[CLASSIFIED MATERIAL REDACTED]

On August 27, 2014, pursuant to 50 U.S.C. §§ 1806(c) and 1825(d), the United States provided notice to the defendant that it "intends to offer into evidence, or otherwise use or disclose in any proceedings in the above-captioned matter, information obtained or derived from electronic surveillance and physical search conducted pursuant to the Foreign Intelligence Surveillance Act of 1978 (FISA), as amended, 50 U.S.C. §§ 1801-1812 and 1821-1829." Doc. 9. On February 2, 2015, the defendant filed, under seal, his motion which seeks, among other things, disclosure of the FISA materials and suppression of the FISA information. Doc. 70.

[CLASSIFIED MATERIAL REDACTED][4]

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

In subsequent sections of this Memorandum, 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); (5) discuss the relevant minimization procedures; and (6) address the defendant's arguments in support of his motion. All of the Government's pleadings and supporting FISA materials are being submitted not only to oppose the defendant's motion, but also to support the United States' request, pursuant to FISA, that this Court: (1) conduct an in camera, ex parte review of the FISA materials; (2) find that the FISA information at issue was lawfully acquired and that the electronic surveillance and physical searches were conducted in conformity with an order of authorization or approval; (3) deny the defendant's request that the FISA information 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]

1. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

2. The FISC's Findings

[CLASSIFIED MATERIAL REDACTED]

II. THE FISA PROCESS

A. OVERVIEW OF FISA

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 searches 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").[5] 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 information is "a significant purpose" of the requested surveillance. 50 U.S.C. § 1804(a)(6)(B).

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

FISA provides that the Attorney General may authorize the emergency employment of electronic surveillance and physical searches 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), 1824(e)(1).[6] Emergency electronic surveillance or physical searches must comport with FISA's minimization requirements, which are discussed below. 50 U.S.C. §§ 1805(e)(2), 1824(e)(2).[7]

---

[6] **[CLASSIFIED MATERIAL REDACTED]**

[7] If no FISC order authorizing the electronic surveillance or physical searches is issued, emergency surveillance or searches 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. See 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 shall cause to be served on any U.S. person named in the application, and

(footnote cont'd on next page)

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 searches, or both, within the United States where a significant purpose is the collection of foreign intelligence information.[8] 50 U.S.C. §§ 1804(a)(6)(B), 1823(a)(6)(B). Under FISA, "[f]oreign intelligence information" means:

> (1) information that relates to, and if concerning a United States person[9] 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

---

others in the FISC's discretion, 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. See 50 U.S.C. § 1806(j); see also 50 U.S.C. § 1824(j)(1) (physical searches). 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 information indicates a threat of death or serious bodily harm. See 50 U.S.C. §§ 1805(e)(5), 1824(e)(5).

[8] **[CLASSIFIED MATERIAL REDACTED]**

[9] **[CLASSIFIED MATERIAL REDACTED]**

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 50 U.S.C. § 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 searches 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;

(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 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).

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 50 U.S.C. § 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 FISC-approved electronic surveillance or physical searches, 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), 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), 1821(4)(c).

[CLASSIFIED MATERIAL REDACTED]

3. Attorney General's Approval

FISA further requires that the Attorney General approve applications for electronic surveillance, physical searches, 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 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. § 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), 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 50 U.S.C. § 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 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
>
> (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); <u>see</u> <u>also</u> 50 U.S.C. § 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), 1824(a)(2)(A). Although protected First Amendment activities cannot form the sole basis for FISC-approved electronic surveillance or physical searches, they may be considered by the FISC if there is other activity indicative 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). 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), 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 approving the electronic surveillance, physical searches, or both, requested in the application. 50 U.S.C. §§ 1805(a), 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 searches targeting a United States person may be approved for up to ninety days, and those targeting a non-United States person may be approved for up to one-hundred and twenty days. 50 U.S.C. §§ 1805(d)(1), 1824(d)(1).[10] 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 searches targeting a United States person may be approved for up to ninety days, and one targeting a non-United States person may be approved for up to one year.[11] 50 U.S.C. §§ 1805(d)(2), 1824(d)(2).

---

[10] **[CLASSIFIED MATERIAL REDACTED]**

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

III. DISTRICT COURT REVIEW OF FISC ORDERS

FISA authorizes the use of information obtained or derived from any FISC-approved electronic surveillance or physical search in a criminal prosecution, 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.[12] 50 U.S.C. §§ 1806(c), (d), 1825(d), (e). 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) that the information was unlawfully acquired; or (2) that 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 or orders or other materials relating to electronic surveillance or physical searches, 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.

[12] An "aggrieved person" is defined as the target of electronic surveillance or "any other person whose communications or activities were subject to electronic surveillance," 50 U.S.C. § 1801(k), as well as "a person whose premises, property, information, or material is the target of physical search" or "whose premises, property, information, or material was subject to physical search. 50 U.S.C. § 1821(2). Gartenlaub is an "aggrieved person" under FISA, and was provided with notice of his status as such and of the Government's intent to use FISA-obtained or -derived information against him at trial.

§§ 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); United States v. Pelton, 835 F.2d 1067, 1075 (4th Cir. 1987).

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

In assessing the legality of FISC-approved electronic surveillance and physical searches, or both, the district court,

> shall, notwithstanding any other law, if the Attorney General files [as he has filed in this proceeding] an affidavit or declaration under oath that disclosure or an adversary hearing would harm the national security of the United States, review in camera and ex parte the application, order, and such other materials relating to the surveillance 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), 1825(g). On the filing of the Attorney General's affidavit or declaration, the court "may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance [or physical search] only

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

where such disclosure is necessary to make an accurate determination of the legality of the surveillance [or search]."[14] 50 U.S.C. §§ 1806(f), 1825(g) (emphasis added). Thus, the propriety of the disclosure of any FISA applications or orders to the 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. Daoud, 755 F.3d 479, 481-82 (7th Cir. 2014); El-Mezain, 664 F.3d at 565; United States v. Abu-Jihaad (Abu-Jihaad II), 630 F.3d 102, 129 (2d Cir. 2010); United States v. Belfield, 692 F.2d 141, 147 (D.C. Cir. 1982); United States v. Nicholson, No. 09-CR-40, 2010 WL 1641167, at *4 (D. Or. Apr. 21, 2010) ("After an in-camera review, the court 'has the discretion to disclose portions of the documents, under appropriate protective procedures, only if [the court] decides that such disclosure is necessary to make an accurate determination of the legality of the surveillance.'") (quoting United States v. Duggan, 743 F.2d 59, 78 (2d Cir. 1984); United States v. Kashmiri, 2010 WL 4705159, at *2 (N.D. Ill. Nov. 10, 2010); United States v. Islamic

[14] In United States v. Warsame, 547 F. Supp. 2d 982, 987 (D. Minn. 2008), the court addressed the meaning of "necessary" in this context: "[t]he legislative history explains that such disclosure is 'necessary' only where the court's initial review indicates that the question of legality may be complicated" by factual misrepresentations, insufficient identification of the target, or failure to comply with the minimization standards in the order.

Am. Relief Agency ("IARA"), No. 07-00087-CR-W-NKL, 2009 WL 5169536, at *3-4 (W.D. Mo. Dec. 21, 2009).

If the district court is able to make an accurate determination of the legality of the electronic surveillance, physical searches, or both, based on its in camera, ex parte review of the materials submitted by the United States, then the court may not order disclosure of any of the FISA materials to the defense, unless otherwise required by due process. Daoud, 755 F.3d 479, 484-85; El-Mezain, 664 F.3d at 566; Duggan, 743 F.2d at 78; Kashmiri, 2010 WL 4705159, at *2.

1. In Camera, Ex Parte Review is the Rule

Federal courts have repeatedly and consistently held that FISA "anticipates that an ex parte, in camera determination is to be the rule," with disclosure and an adversarial hearing being the "exception, occurring only when necessary." Belfield, 692 F.2d at 147 (emphasis in original); accord, El-Mezain, 664 F.3d at 567 ("[D]isclosure of FISA materials is the exception and ex parte, in camera determination is the rule") (citing Abu-Jihaad II, 630 F.3d at 129); Duggan, 743 F.2d at 78; Rosen, 447 F. Supp. 2d at 546; Nicholson, 2010 WL 1641167 at *3-4; United States v. Spanjol, 720 F. Supp. 55, 59 (E.D. Pa. 1989), aff'd, 958 F.2d 365 (3d Cir. 1992).

In fact, every court but one 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.[15] See, e.g., El-Mezain, 664 F.3d at 566 (quoting district court's statement that no court has ever held an adversarial hearing to assist the court); 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 up to that time ordered disclosure of FISA materials); United States v. Isa, 923 F.2d 1300, 1306 (8th Cir. 1991); Spanjol, 720 F. Supp. at 58-59; United States v. Sattar, No. 02-CR-395, 2003 WL 22137012, at *6 (S.D.N.Y. 2003) (citing Nicholson, 955 F. Supp. at 592 & n. 11 (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"); United States. v. Stewart, 590 F.3d 93 (2d Cir. 2009); United States v. Thomson, 752 F. Supp. 75, 79 (W.D.N.Y. 1990); Abu-Jihaad I, 531 F. Supp. 2d at 310; United States v. Mubayyid, 521 F. Supp. 2d 125, 130 (D. Mass. 2007); Rosen, 447 F. Supp. 2d at 546; United States v. Gowadia, No. 05-00486, 2009 WL 1649714, at *2 (D. Haw. June 8, 2009); Kashmiri, 2010 WL 4705159, at *2-3; United States v. Jayyousi, No. 04-60001, 2007 WL 851278, at *7-8 (S.D. Fla. Mar. 15, 2007), aff'd, 657 F.3d 1085 (11th

[15] The district court in United States v. Daoud, No. 12-CR-723 (N.D. Ill. Jan. 29, 2014), ruled that it was capable of making the determination, but nevertheless ordered the disclosure of FISA materials. 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, 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." Daoud, 755 F.3d at 485.

Cir. 2011);[16] United States v. Hassoun, 2007 WL 1068127, *4 (S.D. Fla. April 2, 2007); United States v. Badia, 827 F.2d 1458, 1463 (11th Cir. 1987).

As the Court will see from its examination of the exhibits in the Sealed Appendix, there is nothing extraordinary about the instant FISC-approved electronic surveillance and physical searches that would justify the production and disclosure of highly sensitive and classified material or the suppression of the FISA-obtained or -derived evidence. 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 searches 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 Warsame, 547 F. Supp. 2d at 987 ("issues presented by the FISA applications are straightforward and uncontroversial"); Abu-Jihaad I, 531 F. Supp. 2d at 310; Thomson, 752 F. Supp. at 79. This Court, much like the aforementioned courts, is

[16] All citations to Jayyousi herein are to the Magistrate Judge's Report and Recommendation which was adopted and incorporated into the District Court's Opinion.

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 a high-ranking FBI official 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, 827 F.2d 473, 477 (9th Cir. 1987) ("Congress has a legitimate interest in authorizing the Attorney General to invoke procedures designed to ensure that sensitive security information is not unnecessarily disseminated to anyone not involved in the surveillance operation in question."); accord IARA, 2009 WL 5169536, at *3-4.

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." CIA v. Sims, 471 U.S. 159, 175 (1985); see also Phillippi v. CIA, 655 F.2d 1325, 1332-33 (D.C. Cir. 1981). When a question is raised as to 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, when 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. CIA, 629 F.2d 144, 150 (D.C. Cir. 1980) ("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"). An adversary hearing is not only unnecessary to aid the Court in the straightforward task before it, but such a hearing would create potential dangers that courts have consistently sought to avoid.

As the Belfield court explained:

> Congress recognized the need for the Executive to engage in and employ the fruits of clandestine surveillance without being constantly hamstrung by disclosure requirements. The statute is meant to "reconcile national intelligence and counter-intelligence needs with constitutional principles in a way that is consistent with both national security and individual rights." In FISA the privacy rights of individuals are ensured not through mandatory

> disclosure, but through its provisions for in-depth oversight of FISA surveillance by all three branches of government and by a statutory scheme that to a large degree centers on an expanded conception of minimization that differs from that which governs law enforcement surveillance.

692 F.2d at 148 (footnotes and citations omitted); see also ACLU Found. of So. Cal. v. Barr, 952 F.2d 457, 465 (D.C. Cir. 1991) (citing Belfield for the proposition that Section 1806(f) "is an acceptable means of adjudicating the constitutional rights of persons who have been subjected to FISA surveillance"). As the Daoud court noted, "[e]veryone recognizes that privacy is a legally protectable interest, and it is not an interest of private individuals alone. [FISA] is an attempt to strike a balance between the interest in full openness of legal proceedings and the interest in national security, which requires a degree of secrecy concerning the government's efforts to protect the nation." 755 F.3d at 483.

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 Ninth Circuit. See Ott, 827 F.2d at 476-77 (FISA's review procedures do not deprive a defendant of due process); see also El-Mezain, 664 F.3d at 567; Abu-Jihaad II, 630 F.3d at 117; Spanjol, 720 F. Supp. at 58-59; 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."); Gowadia, 2009 WL 1649714, at *2; Jayyousi, 2007 WL 851278, at *7-8; United States v. Benkahla, 437 F. Supp. 2d 541, 554 (E.D. Va. 2006); ACLU Found., 952 F.2d at 465; 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 defendant's Fourth amendment rights"); United States v. Falvey, 540 F. Supp. 1306, 1315-16 (E.D.N.Y. 1982) (a "massive body of pre-FISA case law of the Supreme Court, [the Second] Circuit and others" supports the conclusion that the legality of electronic surveillance should be determined on an in camera, ex parte basis); Belfield, 692 F.2d at 148-49; Nicholson, 2010 WL 1641167, at *3-4. Another Court in this District has recently conducted an in camera, ex parte review of FISA materials in denying a defendant's motion to suppress FISA information. United States v. Kabir, 5:12-CR-00092-VAP, Doc. No. 277, at 2 (C.D. Cal., May 5, 2014) (CR 277, unpublished order denying motion to suppress FISA information after conducting "a thorough in camera, ex parte examination of the documents contained in the Sealed Appendix, the Government's classified version of the Opposition, and the Attorney General's unclassified Declaration and Claim of Privilege and the classified supporting declarations").

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 in order to determine whether the FISA information was lawfully acquired and whether the surveillance and searches were made in conformity with an order of authorization or approval. Such in camera, ex parte review is the rule in these 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 venue in which to determine whether the FISA information was lawfully acquired and whether the surveillance and searches were made in conformity with an order of authorization or approval.

B. THE DISTRICT COURT'S SUBSTANTIVE REVIEW

1. Standard of Review

In evaluating the legality of the FISA collection, the 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 required by FISA; and (3) whether the collection was properly minimized. See Abu-Jihaad II, 630 F.3d at 130-31. See also 50 U.S.C. §§ 1806(f), 1825(g).

Although federal courts are not in agreement as to whether the probable cause determinations of the FISC should be reviewed de novo or accorded due deference, the material under review here satisfies either standard of review. See Abu-Jihaad II, 630 F.3d at 130 ("Although the established standard of judicial review applicable to FISA warrants is deferential, the government's detailed and complete submissions in this case would easily allow it to clear a higher standard of review.") The Government respectfully submits that it is appropriate to accord due deference to the findings of the FISC, but notes that a number of courts, citing the ex parte nature of the proceedings, have also reviewed the FISC's probable cause determination de novo.[17] While in the minority, other courts, including the Second Circuit in Abu-Jihaad, 630 F.3d at 130, have afforded due deference to the findings of the FISC; accord, United States v. Ahmed, No. 1:06-CR-147, 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. at 236).

In the analogous area of criminal searches and surveillance, the law in the Ninth Circuit, as well as that in other federal circuits, accords great deference to a magistrate judge's probable cause determinations. See, e.g., United States v. Krupa, 658 F.3d 1174,

[17] See, e.g., Kabir, Doc. No. 277, at 2 (in which "the Court engaged in a de novo review of the [FISA] documents); Nicholson, 2010 WL 1641167, *5 (in which a district court in this circuit conducted a de novo review of the FISC's findings of probable cause); 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 (the required showing is "a practical, common-sense decision whether, given all the circumstances set forth in the affidavit . . ., there is a fair probability" that the search will be fruitful (citing Illinois v. Gates, 462 U.S. 231, 238 (1983)); and Kashmiri, 2010 WL 4705159, at *1. In each of these cases, the courts applied a de novo standard in reviewing the FISC's probable cause findings, and each court found the applications before it contained probable cause.

1177 (9th Cir. 2011) ("We review for clear error a magistrate's finding of probable cause to issue an arrest warrant, and give 'great deference' to such findings."); United States v. Hill, 459 F.3d 966, 970 (9th Cir. 2006); see also United States v. Joseph, 709 F.3d 1082, 1093 (11th Cir. 2013) (citing Illinois v. Gates, 462 U.S. at 236); United States v. Robinson, 724 F.3d 878, 884 (7th Cir. 2013). It would thus be consistent for a court that is reviewing FISC-approved electronic surveillance and physical searches to adopt the same posture it would when reviewing the probable cause determination of a criminal search warrant issued pursuant to Rule 41 of the Federal Rules of Criminal Procedure. See Ahmed, 2009 U.S. Dist. LEXIS 120007, at *21-22 (according FISC's probable cause determinations the same deference as a magistrate's criminal probable cause determination); cf. United States v. Cavanagh, 807 F.2d 787, 790 (9th Cir. 1987) (concluding that FISA order can be considered a warrant since it is issued by a detached judicial officer and is based on a reasonable showing of probable cause); In re Sealed Case, 310 F.3d 717, 774 (FISC Ct. Rev. 2002) (declining to decide whether a FISA order constitutes a warrant, but noting "that to the extent a FISA order comes close to meeting Title III, that certainly bears on its reasonableness under the Fourth Amendment"); but Cf. Warsame, 547 F. Supp. 2d at 992 n.10 (noting that the need for foreign intelligence justifies an exception to the warrant requirement).

2. Probable Cause Standard

FISA requires findings of 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, 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. It is this standard - not the standard applicable to criminal search warrants - that this Court must apply. See El-Mezain, 664 F.3d at 564 ("[t]his probable cause standard is different from the standard in the typical criminal case because, rather 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"); Abu-Jihaad II, 630 F.3d at 130-31; Duka, 671 F.3d at 338; Cavanagh, 807 F.2d. at 790 (citing United States v. United States District Court (Keith), 407 U.S. 297, 322 (1972)). This "different, and arguably lower, probable cause standard . . . reflects the purpose for which FISA search orders are issued." Ahmed, 2009 U.S. Dist. LEXIS 120007, at *22.

[CLASSIFIED MATERIAL REDACTED]

3. Standard of Review of Certifications

Certifications submitted in support of a FISA application should be "subjected only to minimal scrutiny by the courts," Badia, 827 F.2d at 1463, 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); United States v.

Sherifi, 793 F. Supp. 2d 751, 760 (E.D.N.C. 2011) ("a presumption of validity [is] accorded to the certifications"); Nicholson, 2010 WL 1641167, at *5 (quoting Rosen, 447 F. Supp. 2d at 545); Warsame, 547 F. Supp. 2d at 990 ("a presumption of validity [is] accorded to the certifications"). 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. Likewise, 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.; see also In re Grand Jury Proceedings, 347 F.3d at 204-05; Badia, 827 F.2d at 1463; Rahman, 861 F. Supp. at 250; IARA, 2009 WL 5169536, at *4; Kashmiri, 2010 WL 4705159, at *1.

The district court's review should determine whether the certifications were made in accordance with FISA's requirements. See United States v. Alwan, No. 1:11-CR-13, 2012 WL 399154, at *7 (W.D. 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; see also Campa, 529 F.3d at 993 ("in the absence of a prima facie showing of a fraudulent statement by the certifying officer, procedural regularity is the only determination to be made if a non-United States person is the target" [quoting Badia, 827 F.2d at 1463]). When the target is a United States person, then the district court should also ensure that each certification is not "clearly erroneous." Id. at 994; Duggan, 743 F.2d at 77; Kashmiri, 2010 WL 4705159, at *2. A "clearly erroneous" finding is established only when "although there is evidence to support it, 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); IARA, 2009 WL 5169536, at *4 (identifying "clearly erroneous" standard of review for FISA certifications).

4. FISA is Subject to the "Good-Faith" Exception

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 in fact met, the Government respectfully submits that the evidence obtained or derived from the FISC-approved electronic surveillance and physical searches is, nonetheless, admissible under the "good faith" exception to the exclusionary rule articulated in United States v. Leon, 468 U.S. 897 (1984).[18] The Seventh Circuit, relying on Leon, held that federal officers were entitled to rely in good faith on a FISA warrant. United States v. Ning Wen, 477 F.3d 896, 897 (7th Cir.

[18] "[E]ven if we were to conclude that amended FISA is unconstitutional, evidence derived from it would nevertheless have been admissible in the government's case. . . . The exclusionary rule precludes the admission of evidence tainted by a Fourth Amendment violation" only in those cases where its application will deter police misconduct. Duka, 671 F.3d at 346 (citing Leon, 468 U.S. at 918).

2007). As the court stated:

> [T]he exclusionary rule must not be applied to evidence seized on the authority of a warrant, even if the warrant turns out to be defective, unless the affidavit supporting the warrant was false or misleading, or probable cause was so transparently missing that "no reasonably well trained officer [would] rely on the warrant."

Id. (quoting Leon) (alteration in original); see also Duggan, 743 F.2d at 77 n.6 (Franks principles apply to review of FISA orders); Ahmed, 2009 U.S. Dist. LEXIS 120007, at *25 n.8, 26-27 ("[t]he FISA evidence obtained . . . would be admissible under Leon's 'good faith' exception to the exclusionary rule were it not otherwise admissible under a valid warrant").

The FISC-approved electronic surveillance and physical searches at issue in this case would fall squarely within this "good faith" exception. As discussed below, notwithstanding the speculation by the defense, 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; see also Massachusetts v. Sheppard, 468 U.S. 981 (1984); United States v. Canfield, 212 F.3d 713, 717-18 (2d Cir. 2000). Further, there are no facts indicating that the FISC failed to act in a neutral and detached manner in authorizing the surveillance and searches at issue. 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 those orders 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 SEARCHES WERE MADE IN CONFORMITY WITH AN ORDER OF AUTHORIZATION OR APPROVAL

[CLASSIFIED MATERIAL REDACTED]

A. THE INSTANT FISA APPLICATIONS MET FISA'S PROBABLE CAUSE STANDARD

[CLASSIFIED MATERIAL REDACTED]

1. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

2. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

3. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

a. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

b. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

c. Conclusion: The Information Acquired From the Targeted Facilities, Places, Property, or Promises 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]

3. Information Not Reasonably Obtainable Through Normal Investigative Techniques

[CLASSIFIED MATERIAL REDACTED]

For all of the above reasons, the FISC correctly found that the certifications were not clearly erroneous.

C. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

D. ALL ELECTRONIC SURVEILLANCE AND PHYSICAL SEARCHES 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 not only that the FISA information was lawfully acquired, but also that the electronic surveillance and physical searches were lawfully conducted. That is, the FISA-obtained or -derived information that will be offered into evidence 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, and all relevant FISC orders.

1. The Standard Minimization Procedures

Once a reviewing court is satisfied that the electronic surveillance or physical searches were properly certified and the information was lawfully acquired pursuant to FISA, it must then examine whether the electronic surveillance or physical searches were lawfully conducted. See 50 U.S.C. §§ 1806(e)(2), 1825(f)(1)(B). In order to examine whether the electronic surveillance or physical searches 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 741; 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 (citing Salameh, 152 F.3d at 154); In re Sealed Case, 310 F.3d at 740-41; 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. 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. Mubayyid, 521 F. Supp. 2d at 134; 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. Thomson, 752 F. Supp. 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 United States 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 ("[t]he minimization requirement obligates the Government to make a good faith effort to minimize the acquisition and retention of irrelevant information"); see also 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), 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 assuming, arguendo, that 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) (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 respectfully submits that it lawfully conducted the FISA-authorized collections discussed herein. Consequently, for the reasons stated above, the Court should find that the FISA-authorized collections discussed herein were lawfully conducted under the minimization procedures approved by the FISC and applicable to the FISA-authorized collections discussed herein.

3. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

V. THE COURT SHOULD REJECT THE DEFENDANT'S LEGAL ARGUMENTS

In his motion, the defendant makes several constitutional claims and requests that the Court: "1) review all FISA applications and warrants, 2) order disclosure of the documents to defense counsel, 3) conduct an evidentiary hearing pursuant to Franks. . . , and 4) as a result, suppress all FISA intercepts and seizures and any fruits derived therefrom."[19] Doc. 70 at p. 28. For the reasons set forth below, the Court should reject the defendant's arguments.

A. THE DEFENDANT'S CONSTITUTIONAL ARGUMENTS LACK MERIT

The defendant raises a number of constitutional challenges, under the First, Fourth, Fifth, and Sixth Amendments, that have repeatedly been rejected by other courts.[20] These arguments lack merit, and the Government will respond to each below.

---

[19] The defendant argues for de novo review by this Court of the FISA materials, or even a review "more exacting than the FISC's review," Doc. 70 at p. 15, a position that has no basis in the law. However, the Government respectfully submits that the Court will find that the FISA-authorized electronic surveillance and physical searches were legally authorized and the FISA information was lawfully acquired, under either de novo review or a due deference review.

[20] The defendant also suggests, without further explanation, that the Government's actions may have been in violation of the Fourteenth Amendment, Doc. 70 at p. 3, which "applies to actions by a State." San Francisco Arts & Athletics, Inc., v. United States Olympic Committee, 483 U.S. 522, 542 n. 21 (1987). The defendant does not allege any State action.

The defendant references the FISA Amendments Act of 2008 and "several controversial programs, such as Prism and Upstream," and

(footnote cont'd on next page)

1. The FISA Applications Were Not Based Solely on Protected First Amendment Activity

[CLASSIFIED MATERIAL REDACTED]

2. The Probable Cause Standard of FISA Complies with the Fourth Amendment's Reasonableness Requirement

The defendant argues that he "has a right to a determination as to whether the most invasive of intrusions into his home violated the Fourth Amendment." Doc. 70 at p. 24. Again, the defendant merely concludes, without factual support, that the Government "may have violated" the Fourth Amendment. Id. at p. 3 (emphasis added). The probable cause threshold that the Government must satisfy before receiving authorization to conduct electronic surveillance or physical searches under FISA complies with the Fourth Amendment's reasonableness standard. The Supreme Court has stated that "[d]ifferent standards may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of the Government for intelligence information and the protected rights of our citizens." Keith, 407 U.S. at 322-23 (recognizing that domestic security surveillance "may involve different policy and practical considerations than the surveillance of 'ordinary crime'"). In Keith, the Supreme Court acknowledged that: (1) the "focus of . . . surveillance [in domestic security investigations] may be less precise than that directed against more conventional types of crime"; (2) unlike ordinary criminal investigations, "[t]he gathering of

---

then concedes that they are not at issue in this case. Doc. 70 at pp. 9-10.

security intelligence is often long range and involves the interrelation of various sources and types of information"; and (3) the "exact targets of such surveillance may be more difficult to identify" than in surveillance operations of ordinary crimes under Title III. Id. Although Keith was decided before FISA's enactment and addressed purely domestic security surveillance, the rationale underlying Keith applies a fortiori to foreign intelligence surveillance, where the Government's interest, at least from a national security perspective, would typically be more pronounced.

FISA was enacted partly in response to Keith. In constructing FISA's framework, Congress addressed Keith's question of whether departures from traditional Fourth Amendment procedures "are reasonable, both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens," and "concluded that such departures are reasonable." See Senate Report at 11. Similarly, many courts - including the Ninth Circuit and the FISC of Review - have relied on Keith in holding that FISA collection conducted pursuant to a FISC order is reasonable under the Fourth Amendment. See Cavanagh, 807 F.2d at 790-91 (holding that FISA satisfies the Fourth Amendment requirements of probable cause and particularity); In re Sealed Case, 310 F.3d at 738, 746 (finding that while many of FISA's requirements differ from those in Title III, few of those differences have constitutional relevance); Duggan, 743 F.2d at 74 (holding that FISA does not violate the Fourth Amendment); see also Ning Wen, 477 F.3d at 898 (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); Pelton, 835 F.2d at 1075 (finding FISA's procedures compatible with the Fourth Amendment); Warsame, 547 F. Supp. 2d at 993-94 (holding that FISA's probable cause and particularity requirements satisfy the reasonableness requirement of the Fourth Amendment); Mubayyid, 521 F. Supp. 2d at 135-41 (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).

3. The Court's In Camera and Ex Parte Review Comports with the Fifth Amendment's Due Process and the Sixth Amendment's Counsel and Confrontation Clauses

The defendant states that "[u]nder the Fifth Amendment's Due Process Clause, defendants must be afforded a process that permits them to seek the suppression remedy," Doc. 70 at p. 24, but fails to explain how he has been denied that remedy here, where FISA expressly provides a statutory suppression remedy, 50 U.S.C. §§ 1806(e), 1825(f), of which he has availed himself by filing this motion. Citing to authorities that did not address FISA, the defendant further argues that "[t]he Court's review in camera is not a substitute for the defense counsel's participation," and that without such participation he "is not receiving the Sixth Amendment constitutional benefit of adequate representation of counsel." Doc.

70 at p. 27. Accordingly, the defendant claims, under the "Sixth Amendment and/or the Due Process clause, disclosure of the FISA materials is authorized and appropriate in this case." Id.

Several District Courts in the Ninth Circuit have addressed the right to confrontation in this context and found that "FISA's in camera review provisions have been held to be constitutional." Nicholson, 2010 U.S. Dist. LEXIS 45126, citing Isa, 923 F.2d at 1037-08 (Sixth Amendment right of confrontation is not violated by FISA's in camera review procedure); see also United States v. Lahiji, 2013 WL 550492 (D. Or. February 12, 2013), *4 (Court found no violation of defendants' Fourth, Fifth, or Sixth Amendment rights); United States v. Jamal, 2011 U.S. Dist. LEXIS 12224 (D. Az. February 11, 2011), *5 (Movant's Sixth Amendment rights were not violated by trial counsel's inability to discuss FISA materials); United States v. Hussein, 2014 WL 1682845 (S.D. Cal. April 29, 2014), *3 (the "in camera, ex parte review process under FISA satisfies due process under the United States Constitution").

A Sixth Amendment argument similar to the defendant's was advanced unsuccessfully in Warsame, 547 F. Supp. 2d at 988 n.4 (finding argument "without merit" and citing to Nicholson, 955 F. Supp. at 592). Other courts have also consistently rejected the Sixth Amendment argument. See Belfield, 692 F.2d at 148 (rejecting Sixth Amendment challenge); Isa, 923 F.2d at 1306-07 (rejecting Sixth Amendment challenge); Megahey, 553 F. Supp. at 1193 (rejecting Sixth Amendment challenge); Benkhala, 437 F. Supp. 2d at 554 (rejecting

Sixth Amendment right to counsel challenge); Falvey, 540 F. Supp. at 1315-16 (rejecting First, Fifth, and Sixth Amendment challenges and noting that a "massive body of pre-FISA case law of the Supreme Court, [the Second] Circuit and others" supports the conclusion that the legality of electronic surveillance should be determined on an in camera, ex parte basis). In overturning a district court's order to disclose FISA materials to the defense, the Daoud court described the belief that "adversary procedure is always essential to resolve contested issues of fact" as "an incomplete description of the American legal system in general and the federal judicial system in particular." 755 F.3d at 482.

B. THE DEFENDANT HAS NOT ESTABLISHED ANY BASIS TO DISCLOSE THE FISA MATERIALS

In support of his argument to disclose the FISA materials, the defendant asserts that: (1) there is "a significant question about whether any need for secrecy persists" with regard to the FISA materials (Doc. 70 at p. 12); and (2) the affiant in the FISA materials "intentionally or recklessly made materially false statements and/or omitted material information . . . ."[21] Doc. 70 at p. 14. On these bases, the defendant seeks the disclosure of classified FISA materials, which are protected from such disclosure, except as provided in 50 U.S.C. §§ 1806(f)-(g) and 1825(g)-(h). As discussed below, Congress's clear intention is that FISA materials should be

---

[21] **[CLASSIFIED MATERIAL REDACTED]**

reviewed in camera and ex parte and in a manner consistent with the realities of modern intelligence needs and investigative techniques. Indeed, this Court will find upon its own review that there is nothing extraordinary about this case that would prompt this Court to order the disclosure of highly sensitive and classified FISA materials and that the defendant has failed to present any colorable basis for the Court to order disclosure of the FISA materials.

There is only one reason to disclose the FISA materials to defense counsel. The Court must conduct its review of those materials in camera and ex parte, and disclosure is within the Court's discretion only following that review and only if the Court is unable to determine the legality of the electronic surveillance, physical searches, or both, without the assistance of defense counsel. 50 U.S.C. §§ 1806(f), 1825(g). Duggan, 743 F.2d at 78; see also Daoud, 755 F.3d at 482. Duggan's holding is fully supported by the legislative history of Section 1806(f) of FISA, which states: "The court may order disclosure to [the defense] only if it finds that such disclosure is necessary to make an accurate determination of the legality of the surveillance . . . Once a judicial determination is made that the surveillance was lawful, a motion for discovery . . . must be denied." Senate Report at 64-65.

The defendant seeks the "opportunity to prove that the affiant intentionally or recklessly made materially false statements and/or omitted material information from the FISA applications." Doc. 70 at p. 14. However, FISA's plain language precludes defense counsel from accessing the classified FISA materials to conduct a fishing expedition. In Medunjanin, the court noted that "[d]efense counsel . . . may not inspect the FISA dockets to construct a better argument for inspecting the FISA dockets. Such a circular exercise would be patently inconsistent with FISA . . . ." 2012 WL 526428 at *10. See Badia, 827 F.2d at 1462 (rejecting the defendant's request for "disclosure of the FISA application, ostensibly so that he may review it for errors").

The defendant asserts that disclosure is necessary as it is "impossible for the Court and government counsel to review the purportedly secret documents and determine if additional things of this nature, those things personal to [him], were correct." Doc. 70 at p. 27. However, as this Court will see from its review, the FISA materials are presented in a well-organized and straightforward manner that will allow the Court to make its determination of the lawfulness of the FISA collection without seeking input from defense counsel. Again, defendant's claim that the Court would need assistance from defense counsel is merely an attempt to circumvent the clear language of the statute. See 50 U.S.C. §§ 1806(f), 1825(g). As the Belfield court stated: "Congress was adamant, in enacting FISA, that [its] 'carefully drawn procedure[s]' are not to be bypassed." Belfield, 692 F.2d at 146 (citing Senate Report at 63); see also United States v. Mohamud, 2014 WL 2866749, *32 (D.Or., June 24, 2014) ("[o]bviously it would be helpful to the court to have defense counsel review the materials prior to making arguments.

Congress, however, did not put 'helpful' in the statute; it chose 'necessary.'") As the Daoud Court stated, "the defendant's misreading of the statute" would circumvent the required in camera, ex parte review whenever a defense counsel "believed disclosure necessary, since if the judge does not conduct the ex parte review, she will have no basis for doubting the lawyer's claim of necessity." 755 F.3d at 842.

[CLASSIFIED MATERIAL REDACTED]

The defendant's arguments in support of disclosure of the FISA materials have no basis in the law, and disclosure of the FISA materials would cause exceptionally grave damage to the national security. In summary, the defendant is not entitled to the FISA materials for the purpose of challenging the lawfulness of the FISA authorities and the complete record presented to the FISC has been provided to this Court in well-organized and straightforward manner, obviating the defendant's claim that this Court would not be able to review and make a determination as to the legality of the FISA collection without the assistance of defense counsel.

C. THE DEFENDANT HAS NOT ESTABLISHED ANY BASIS FOR THE COURT TO CONDUCT A FRANKS HEARING

The defendant alleges that the "FISA applications likely contain intentional or reckless material falsehoods or omissions, and therefore violate the Fourth Amendment principles identified in Franks . . . ," and requests that the Court conduct a Franks hearing. Doc. 70 at pp. 2-4. The Court should decline to hold such a hearing.

To merit a Franks hearing, a defendant must make a "concrete and substantial preliminary showing" that the affiant deliberately or recklessly included false statements, or failed to include material information, in the affidavit, and that the resulting misrepresentation was essential to the finding of probable cause. Franks, 438 U.S. at 155-56; United States v. Craighead, 539 F.3d 1073, 1080 (9th Cir. 2008). The Franks threshold is not met even by an offer of proof of an impropriety that might have affected the outcome of the probable cause determination, but rather requires one that was "necessary to the finding of probable cause." United States v. Colkley, 899 F.2d 297, 301-02 (4th Cir. 1990); see also United States v. Shnewer, 2008 U.S. Dist. LEXIS 112001, at 38 (2009) ("[E]ven if the Court were to determine there existed a reckless or intentional falsehood or omission in the FISA application materials, the evidence obtained still should not be suppressed unless the Court makes the further finding that the falsehood or omission was material to the probable cause determination.").

Only after a defendant makes the requisite showing[22] may the Court conduct a Franks hearing to determine if there are material

[22] Indeed, even if a defendant offers sufficient proof to show that an affidavit involved false statements or omissions, a hearing should not be held where the affidavit would still provide probable cause if the allegedly false material were eliminated, or if the allegedly omitted information were included. Franks, 438 U.S. at 171; Colkley, 899 F.2d at 300; United States v. Ketzeback, 358 F.3d 987, 990 (8th Cir. 2004); United States v. Martin, 615 F.2d 318, 328 (5th Cir. 1980).

misrepresentations of fact, or omissions of material fact, in the FISA applications sufficient to warrant suppression of the FISA-obtained or -derived evidence. Franks, 438 U.S. at 171. The defendant, however, ignores this burden and simply incorporates by reference his Motion to Traverse Search Warrants SA14-315M, SA14-316M, SA14-317M, and SA14-318M, and Request for Franks Hearing (Doc. 73) (hereinafter, "Motion to Traverse").[23] He speculates that, because the FISA applications "presumably present[] much of the same information" as an affidavit supporting one of the criminal search warrants, the FISA applications must have contained "serious misrepresentations and omissions." Doc. 70 at pp. 13-14.

[CLASSIFIED MATERIAL REDACTED]

As noted supra, the defendant seeks the "opportunity to prove that the affiant intentionally or recklessly made materially false statements and/or omitted material information from the FISA applications," Doc. 70 at p. 14, which would allow him, and defendants in every case, to obtain the FISA materials by merely alleging some impropriety.[24] Disclosing FISA materials to defendants would then become the rule, violating Congress' clear intention, set

[23] In response to the defendant's challenges to the criminal search warrants, the Government filed a Consolidated Opposition to Defendant's Motion to Traverse and to Quash Search Warrant at the time this response was filed.

[24] The Hon. Josephine Staton Tucker in this district referred to this as "backwards reasoning" in denying a defendant's motion to suppress FISA-derived evidence. United States v. Mihalik, 11-CR-833(A), Doc. No. 108, at 2 (C.D. Cal., Oct. 3, 2012) (Minute Order Denying Defendant's Motion to Suppress FISA Derived Evidence).

forth in 50 U.S.C. §§ 1806(f) and 1825(g), that the FISA materials be reviewed in camera and ex parte in a manner consistent with the realities of modern intelligence needs and investigative techniques. Courts have acknowledged that the FISA statute does not envision such disclosure without establishing a basis for it. In Belfield, for example, the court noted that "Congress was also aware of these difficulties [faced by defense counsel without access to FISA materials and] chose to resolve them through means other than mandatory disclosure." Belfield, 692 F.2d at 148. As Judge Leinenweber framed the difficulty facing defense counsel:

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

Kashmiri, 2010 U.S. Dist. LEXIS 119470, at * 17.

Moreover, courts have rejected other defendants' attempts to force a Franks hearing by positing unsupported speculation to challenge the validity of FISC orders, and this Court should do so here. See Abu-Jihaad, 531 F. Supp. 2d at 309; Hassoun, 2007 WL 1068127 at *4; Mubayyid, 521 F. Supp. 2d at 130-31; Kashmiri, 2010 U.S. Dist. LEXIS 119470, at *17 (noting that the court "has already undertaken a process akin to a Franks hearing through its ex parte, in camera review"); Shnewer, 2008 U.S. Dist. LEXIS 112001, at 37

("This catch-22 has not troubled courts, however, and they defer to FISA's statutory scheme."); Mubayyid, 521 F. Supp. 2d at 131 ("The balance struck under FISA--which is intended to permit the gathering of foreign intelligence under conditions of strict secrecy, while providing for judicial review and other appropriate safeguards--would be substantially undermined if criminal defendants were granted a right of disclosure simply to ensure against the possibility of a Franks violation.").[25]

The defendant has failed to carry the burden of establishing the prerequisites for a Franks hearing, and his attempt to obtain disclosure of the FISA materials to meet that burden is unprecedented and runs counter to the plain language of FISA, the clear directive of the Franks court itself, and the intent of Congress. The defendant's failure to make a threshold showing of a falsehood in the FISA applications is fatal to a Franks motion. For these reasons, the Court should therefore deny the defendant's request for a Franks hearing and his request for disclosure of the FISA materials.

D. THE DEFENDANT HAS NOT ESTABLISHED ANY BASIS FOR THE COURT TO SUPPRESS THE FISA INFORMATION

The defendant requests in his motion that the Court suppress any evidence obtained or derived from searches or surveillance conducted pursuant to FISA (i.e., the FISA information). Doc. 70 at p. 4. In

---

[25] The defendant ignores this balance, claiming that "the focus must now be on the rights of the defendant, rather than general interests of intelligence gathering." Doc. 70 at p. 15. His approach contravenes FISA, which was carefully drafted to take both considerations into account.

support of this argument, the defendant alleges that the Government "may" have committed various improprieties. Id. at pp. 2-3.

[CLASSIFIED MATERIAL REDACTED]

As the Court will see from its ex parte, in camera review of the FISA materials, the Government complied with all of FISA's statutory requirements. Accordingly, the Government submits that there is no basis to suppress the FISA information in the present case.

VI. CONCLUSION: THERE IS NO BASIS FOR THE COURT TO DISCLOSE THE FISA MATERIALS, TO CONDUCT A FRANKS HEARING, OR TO SUPPRESS THE FISA INFORMATION

The defendant's Motion should be denied in its entirety. FISA's provisions for in camera, ex parte review comport with the due process requirements of the United States Constitution. See, e.g., Spanjol, 720 F. Supp. at 58-59; United States v. Butenko, 494 F.2d 593, 607 (3d Cir.), cert denied sub nom Ivanov v. United States, 419 U.S. 881 (1974); Damrah, 412 F.3d at 624; Warsame, 547 F. Supp. 2d at 988-89. The defendant advances no argument to justify any deviation from these well-established precedents.

The Attorney General has filed a declaration in this case stating that disclosure of the FISA materials or an adversary hearing 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 the electronic surveillance and physical searches 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 proper standard for disclosure; that is, only where the Court determines that disclosure is necessary to the Court's accurate determination of the legality of the FISA collection.

The Court can make this determination without disclosing the classified and highly sensitive FISA materials to the defendant. The FISA materials at issue here 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 has failed to present any colorable basis for supplanting Congress' reasoned judgment with a different proposed standard of review.

[CLASSIFIED MATERIAL REDACTED]

Even if this Court were to determine that the acquisition of the FISA information had not been lawfully acquired or that the electronic surveillance was 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 (holding that the Leon good-faith exception applies to FISA orders); Mubayyid, 521 F. Supp. 2d at 140 n. 12 (noting that the Government could proceed in good-faith reliance on FISA orders even if FISA were deemed unconstitutional); Ahmed, 2009 U.S. Dist. LEXIS 120007, at *25 n. 8; Nicholson, 2010 WL 1641167, at *6.

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 searches at issue in this case were both lawfully authorized and lawfully conducted; (2) hold that disclosure to the defendant of the FISA materials and the Government's classified submission is not authorized because the Court is able to make an accurate determination of the legality of the electronic surveillance and physical searches without disclosing the FISA materials or any portions thereof; (3) hold that the fruits of electronic surveillance, physical searches, or both, should not be suppressed; (4) order that the FISA materials and the Government's classified submissions be maintained under seal by the Court Security Officer or

//

//

//

//

his or her designee; and (5) deny the defendant's Motion without an evidentiary hearing.[26]

DATED: May 4, 2015

Respectfully submitted,

STEPHANIE YONEKURA
Acting United States Attorney

/s/
ANTHONY LEWIS
Assistant United States Attorney

CASEY ARROWOOD
Trial Attorney
Counterespionage Section
National Security Division

[26] A district court order granting motions or requests under 50 U.S.C. §§ 1806(g) or 1825(h), a decision that electronic surveillance or physical searches were not lawfully authorized or conducted, and an order requiring the disclosure of FISA materials is 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.