

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

UNITED STATES OF AMERICA,)	FILED WITH CLASSIFIED
Plaintiff,)	INFORMATION SECURITY
)	OFFICER
v.)	
)	CASE NO. 12-CR-723
ADEL DAOUD,)	
Defendant.)	<i>IN CAMERA,</i>
)	<i>EX PARTE</i>
)	UNDER SEAL

**GOVERNMENT'S UNCLASSIFIED MEMORANDUM IN OPPOSITION
TO DEFENDANT'S MOTION FOR DISCLOSURE OF FISA-RELATED
MATERIAL AND TO SUPPRESS THE FRUITS OR DERIVATIVES OF
ELECTRONIC SURVEILLANCE AND ANY OTHER MEANS OF
COLLECTION CONDUCTED PURSUANT TO FISA OR OTHER
FOREIGN INTELLIGENCE GATHERING**

TABLE OF CONTENTS

I.	Introduction.....	1
A.	Background.....	3
B.	Overview of the FISA Authorities	5
	1. [CLASSIFIED MATERIAL REDACTED]	
	2. The FISC’s Findings.....	5
II.	The FISA Process.....	5
A.	Overview of FISA.....	5
B.	The FISA Application.....	7
	1. The Certification.....	9
	2. Minimization Procedures	10
	3. Attorney General’s Approval	11
C.	The FISC’s Orders	11
III.	The District Court’s Review of FISC Orders	16
A.	The Review Is to Be Conducted <i>in Camera</i> and <i>ex Parte</i>	17
	1. <i>In Camera, Ex Parte</i> Review is the Rule	19
	2. <i>In Camera, Ex Parte</i> Review is Constitutional	23
B.	The District Court’s Substantive Review	25
	1. Standard of Review of Probable Cause.....	25
	2. Standard of Review of Certifications.....	28
	3. FISA is Subject to the “Good-Faith” Exception.....	29
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	31
A.	The Instant FISA Applications Met FISA’s Probable Cause Standard	31
	1. [CLASSIFIED MATERIAL REDACTED]	
	2. [CLASSIFIED MATERIAL REDACTED]	
	a. [CLASSIFIED MATERIAL REDACTED]	
	b. [CLASSIFIED MATERIAL REDACTED]	
	c. [CLASSIFIED MATERIAL REDACTED]	
	d. [CLASSIFIED MATERIAL REDACTED]	
	e. [CLASSIFIED MATERIAL REDACTED]	
	f. [CLASSIFIED MATERIAL REDACTED]	
	g. [CLASSIFIED MATERIAL REDACTED]	
	3. [CLASSIFIED MATERIAL REDACTED]	

a.	[CLASSIFIED MATERIAL REDACTED]	
b.	[CLASSIFIED MATERIAL REDACTED]	
c.	[CLASSIFIED MATERIAL REDACTED]	
d.	[CLASSIFIED MATERIAL REDACTED]	
e.	[CLASSIFIED MATERIAL REDACTED]	
f.	[CLASSIFIED MATERIAL REDACTED]	
g.	[CLASSIFIED MATERIAL REDACTED]	
h.	[CLASSIFIED MATERIAL REDACTED]	
i.	Conclusion: The Information Acquired from the Targeted Facilities, Places, Property, or Promises Was Lawfully Acquired.....	33
B.	The Certifications Complied with FISA.....	33
1.	Foreign Intelligence Information.....	33
2.	“A Significant Purpose”.....	33
3.	Information Not Reasonably Obtainable Through Normal Investigative Techniques.....	33
C.	All Electronic Surveillance and Physical Searches Were Conducted in Conformity with an Order of Authorization or Approval.....	34
1.	The Standard Minimization Procedures.....	34
2.	The FISA Information Was Appropriately Minimized.....	39
V.	The Court Should Reject the Defendant’s Legal Arguments.....	40
A.	The Defendant Has Not Established any Basis for the Court to Disclose FISA Materials to Him.....	41
1.	Due Process Does Not Require Disclosure of the FISA Materials.....	41
2.	<i>Franks v. Delaware</i> Does Not Require Disclosure of FISA Materials.....	43
3.	Daoud’s Age Does Not Necessitate Disclosure.....	47
4.	There Is No Basis for Disclosure Related to the FISA Amendments Act of 2008.....	48
B.	The Defendant Has Not Established Any Basis for the Court to Suppress the FISA-Acquired Evidence.....	49
1.	The Government Satisfied the Probable Cause Requirements under FISA.....	49
a.	[CLASSIFIED MATERIAL REDACTED]	
b.	“Raw Intelligence” Is Not Inherently Unreliable.....	50

2.	There Is No Basis for Suppression Related to the FISA Amendments Act of 2008.....	51
3.	The FISA Surveillance in Question Was Not Conducted Solely on Daoud's Protected First Amendment Activity.....	51
4.	A Significant Purpose of the FISA Surveillance Was the Collection of Foreign Intelligence Information	52
C.	FISA's Significant Purpose Standard Complies with the Requirements of the Fourth Amendment	52
VI.	Conclusion	58

TABLE OF AUTHORITIES

FEDERAL CASES

<i>ACLU Found. of So. Cal. v. Barr</i> , 952 F.2d 457 (D.C. Cir. 1991)	23
<i>Alsabri v. Obama</i> , 764 F. Supp. 2d 60 (D.D.C. 2011)	51
<i>Bensayah v. Obama</i> , 610 F.3d 718 (D.C. Cir. 2010)	50
<i>CIA v. Sims</i> , 471 U.S. 159 (1985)	22, 22
<i>Clapper v. Amnesty Int’l USA</i> , 133 S. Ct. 1138 (2013)	1
<i>Franks v. Delaware</i> , 438 U.S. 154 (1978)	1, 28, 40, 43–47
<i>Halperin v. CIA</i> , 629 F.2d 144 (D.C. Cir. 1980)	22
<i>Illinois v. Gates</i> , 462 U.S. 213 (1983)	26, 26
<i>In re Kevork</i> , 634 F. Supp. 1002 (C.D. Cal. 1985), <i>aff’d</i> , 788 F.2d 566 (9th Cir. 1986)	21
<i>In re Sealed Case</i> , 310 F.3d 717 (FISA Ct. Rev. 2002)	27, 35, 56
<i>Khan v. Obama</i> , 741 F. Supp. 2d 1 (D.D.C. 2010)	50
<i>Khan v. Obama</i> , 655 F.3d 20 (D.C. Cir. 2011)	51
<i>Los Angeles Cnty. v. Davis</i> , 440 U.S. 625 (1979)	56

<i>Massachusetts v. Sheppard</i> , 468 U.S. 981 (1984)	30
<i>Mayfield v. United States</i> , 504 F. Supp. 2d 1023 (D. Or. 2007), <i>vacated</i> , 599 F.3d 964 (9th Cir. 2010)	56
<i>Mayfield v. United States</i> , 599 F.3d 964 (9th Cir. 2010)	56
<i>Parhat v. Gates</i> , 532 F.3d 834 (D.C. Cir. 2008)	50
<i>Phillippi v. CIA</i> , 655 F.2d 1325 (D.C. Cir. 1981)	21
<i>Scott v. United States</i> , 436 U.S. 128 (1978)	38
<i>United States v. Abu-Jihaad</i> , 531 F. Supp. 2d 299 (D. Conn. 2008), <i>aff'd</i> , 630 F.3d 102 (2d Cir. 2010)	<i>passim</i>
<i>United States v. Ahmed</i> , No. 1:06-CR-147, 2009 U.S. Dist. Lexis 120007 (N.D. Ga. Mar. 19, 2009)	25, 26, 28, 29-30, 42, 59
<i>United States v. Alwan</i> , No. 1:11-CR-13, 2012 WL 399154 (W.D. Ky. Feb. 7, 2012)	29
<i>United States v. Badia</i> , 827 F.2d 1458 (11th Cir. 1987)	20, 28-29, 54
<i>United States v. Belfield</i> , 692 F.2d 141 (D.C. Cir. 1982)	18, 19, 21, 23-24, 42, 46
<i>United States v. Benkahla</i> , 437 F. Supp. 2d 541 (E.D. Va. 2006)	24, 42, 56
<i>United States v. Bin Laden</i> , 126 F. Supp. 2d 264 (S.D.N.Y. 2000)	35-36

<i>United States v. Butenko</i> , 494 F.2d 593 (3th Cir. 1974), <i>cert. denied sub nom.</i> <i>Ivanov v. United States</i> , 419 U.S. 881 (1974).....	58
<i>United States v. Campa</i> , 529 F.3d 980 (11th Cir. 2008)	29
<i>United States v. Canfield</i> , 212 F.3d 713 (2d Cir. 2000)	30
<i>United States v. Carson</i> , 582 F.3d 827 (7th Cir. 2009)	26
<i>United States v. Cavanagh</i> , 807 F.2d 787 (9th Cir. 1987)	27, 27
<i>United States v. Colkley</i> , 899 F.2d 297 (4th Cir. 1990)	44-45
<i>United States v. Damrah</i> , 412 F.3d 618 (6th Cir. 2005)	24, 58
<i>United States v. Duggan</i> , 743 F.2d 59 (2d Cir. 1984)	18, 28, 29, 30, 45, 54
<i>United States v. Duka</i> , 671 F.3d 329 (3d Cir. 2011)	17, 27, 30
<i>United States v. Dumeisi</i> , 424 F.3d 526 (7th Cir. 2005)	26
<i>United States v. El-Mezain</i> , 664 F.3d 467 (5th Cir. 2011)	<i>passim</i>
<i>United States v. Falcone</i> , 364 F. Supp. 877, 886 (D.N.J. 1973), <i>aff'd</i> , 500 F.2d 1401 (3rd Cir. 1974).....	39-39
<i>United States v. Falvey</i> , 540 F. Supp. 1306 (E.D.N.Y. 1982).....	24, 42
<i>United States v. Garcia</i> , 413 F.3d 201 (2d Cir. 2005)	29

<i>United States v. Gowadia</i> , No. 05-00486, 2009 WL 1649714 (D. Haw. June 8, 2009)	20, 24
<i>United States v. Hammoud</i> , 381 F.3d 316 (4th Cir. 2004), rev'd on other grounds, 543 U.S. 1097 (2005), <i>op. reinstated in pertinent part</i> , 405 F.3d 1034 (4th Cir. 2005)	26, 36, 37, 38
<i>United States v. Hassoun</i> , No. 04-60001, 2007 WL 1068127 (S.D. Fla. Apr. 4, 2007)	20, 47
<i>United States v. Isa</i> , 923 F.2d 1300 (8th Cir. 1991)	20, 38, 42
<i>United States v. Islamic Am. Relief Agency</i> , No. 07-00087-CR-W-NKL, 2009 WL 5169536 (W.D. Mo. Dec. 21, 2009)	18
<i>United States v. Jayyousi</i> , No. 04-60001, 2007 WL 851278 (S.D. Fla. Mar. 15, 2007), <i>aff'd</i> , 657 F.3d 1085 (11th Cir. 2011)	20, 24, 56
<i>United States v. Jeffus</i> , 22 F.3d 554 (4th Cir. 1994)	45
<i>United States v. Johnson</i> , 952 F.2d 565 (1st Cir. 1991)	54-55
<i>United States v. Kashmiri</i> , No. 09-CR-830-4, 2010 WL 4705159 (N.D. Ill. Nov. 10, 2010)	18-20, 26, 29, 44-47, 56
<i>United States v. Ketzeback</i> , 358 F.3d 987 (8th Cir. 2004)	46
<i>United States v. Leon</i> , 468 U.S. 897 (1984)	29-30, 58
<i>United States v. Martin</i> , 615 F.2d. 318 (5th Cir. 1980)	46

<i>United States v. Marzook</i> , 435 F. Supp. 2d 778 (N.D. Ill. 2006)	56
<i>United States v. McIntire</i> , 516 F.3d 576 (7th Cir. 2008)	26
<i>United States v. Medunjanin</i> , No. 10-CR-19-1, 2012 WL 526428 (S.D.N.Y. Feb. 16, 2012)	39
<i>United States v. Megahey</i> , 553 F. Supp. 1180 (E.D.N.Y. 1982)	24, 42
<i>United States v. Mubayyid</i> , 521 F. Supp. 2d 125 (D. Mass. 2007)	20, 36, 38, 45, 47, 56, 59
<i>United States v. Nicholson</i> , No. 09-CR-40, 2010 WL 1641167 (D. Or. Apr. 21, 2010)	18-19, 24-26, 28, 59
<i>United States v. Nicholson</i> , 955 F. Supp. 588 (E.D. Va. 1997)	20, 42
<i>United States v. Ning Wen</i> , 477 F.3d 896 (7th Cir. 2007)	30, 56, 58
<i>United States v. Ott</i> , 827 F.2d 473 (9th Cir. 1987)	21, 24
<i>United States v. Pelton</i> , 835 F.2d 1067 (4th Cir. 1987)	17, 54
<i>United States v. Rahman</i> , 861 F. Supp. 247 (S.D.N.Y. 1994), <i>aff'd</i> , 189 F.3d 88 (2d Cir. 1999)	14, 28, 35, 36, 52
<i>United States v. Robinson</i> , 724 F.3d 878 (7th Cir. 2013)	26
<i>United States v. Rosen</i> , 447 F. Supp. 2d 538 (E.D. Va. 2006)	14, 19, 26, 28, 36, 52
<i>United States v. Salameh</i> , 152 F.3d 88 (2d Cir. 1998)	35

<i>United States v. Sarkissian</i> , 841 F.2d 959 (9th Cir. 1988)	55
<i>United States v. Sattar</i> , No. 02-CR-395, 2003 WL 22137012 (S.D.N.Y. 2003)	20
<i>United States v. Sherifi</i> , 793 F. Supp. 2d 751 (E.D.N.C. 2011)	28, 57
<i>United States v. Spanjol</i> , 720 F. Supp. 55 (E.D. Pa. 1989), <i>aff'd</i> , 958 F.2d 365 (3d Cir. 1992)	19-20, 24, 58
<i>United States v. Stewart</i> , 590 F.3d 93 (2d Cir. 2009)	20
<i>United States v. Truong Dinh Hung</i> , 629 F.2d 908 (4th Cir. 1980)	54-54, 56
<i>United States v. Thomson</i> , 752 F. Supp. 75 (W.D.N.Y. 1990)	20, 21, 35, 37
<i>United States v. United States District Court (Keith)</i> , 407 U.S. 297 (1972)	27, 37, 57
<i>United States v. U.S. Gypsum Co.</i> , 333 U.S. 364 (1948)	28
<i>United States v. Warsame</i> , 547 F. Supp. 2d 982 (D. Minn. 2008)	<i>passim</i>
<i>United States v. Yunis</i> , 867 F.2d 617 (D.C. Cir. 1989)	22

U.S. CONSTITUTION

Amend. I	14, 40, 51
Amend. IV	<i>passim</i>
Amend. VI	42

FEDERAL STATUTES

50 U.S.C. § 1801	<i>passim</i>
50 U.S.C. §§ 1801-1812	1
50 U.S.C. § 1803	5
50 U.S.C. § 1804	6, 7, 9-10, 53
50 U.S.C. § 1805	7, 12, 14, 52
50 U.S.C. § 1806	<i>passim</i>
50 U.S.C. § 1821	<i>passim</i>
50 U.S.C. §§ 1821-1829	1
50 U.S.C. § 1823	7, 9-10
50 U.S.C. § 1824	7, 12, 14, 52
50 U.S.C. § 1825	<i>passim</i>
50 U.S.C. § 1881	<i>passim</i>
FISA Amendments Act of 2008, Pub. L. 110-261, 122 Stat. 2436 (2008)	48-49, 51
Immigration and Nationality Act, § 101(a)(20)	7
Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (“PATRIOT Act”), Pub. L. No. 107-56, 115 Stat. 272 (2001)	6, 53, 56

OTHER AUTHORITIES

Fed. R. Crim. P. 41	27
H.R. Rep. No. 95-1283, 95th Cong., 2d Sess., Pt. 1 (1978)	36-37, 39
S. Rep. No. 95-701, 95th Cong., 2d Sess. (1978)	37-38

I. INTRODUCTION

The Government is filing this classified memorandum in opposition to defendant Adel Daoud's "Motion for Disclosure of FISA-Related Material and to Suppress the Fruits or Derivatives of Electronic Surveillance and Any other Means of Collection Conducted Pursuant to FISA or Other Foreign Intelligence Gathering" (hereinafter, "defendant's motion"). (DE 51). In essence, the defendant's motion seeks: (1) disclosure of all applications, orders, and related materials filed with the Foreign Intelligence Surveillance Court ("FISC") (the "FISA materials");¹ (2) suppression of information obtained or derived pursuant to FISA; and (3) the Court to require an evidentiary hearing pursuant to *Franks v. Delaware*, 438 U.S. 154 (1978). (DE 51, at 4).

The defendant's motion has triggered this Court's review of the FISA materials related to the FISA-authorized² electronic surveillance and physical searches³ of him to determine whether the FISA information was lawfully acquired and whether the electronic surveillance and physical searches were made in

¹ [CLASSIFIED MATERIAL REDACTED]

² [CLASSIFIED MATERIAL REDACTED]

³ The provisions of FISA that address electronic surveillance being used against the defendant in this case are found at 50 U.S.C. §§ 1801-1812; those that address physical searches being used against the defendant in this case are found at 50 U.S.C. §§ 1821-1829. As discussed *infra*, the Supreme Court has referred to these sections of FISA as "traditional FISA." *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1144 (2013). 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.

conformity with an order of authorization or approval (*i.e.*, were “lawfully authorized and lawfully conducted”). Whenever “any motion or request is made by an aggrieved person pursuant to any other statute or rule of the United States . . . before any . . . other authority of the United States . . . to discover or obtain applications or orders or other materials relating to” FISA-authorized electronic surveillance, physical searches, or both, the Government may file an affidavit under oath in which the Attorney General claims that disclosure or an adversary hearing would harm the national security of the United States and the Court shall then review the FISA materials *in camera* and *ex parte*.⁴ 50 U.S.C. §§ 1806(f), 1825(g). The Government respectfully submits that, for the reasons set forth hereinafter, this Court should conduct an *in camera*, *ex parte* review of the documents relevant to the defendant’s motion in accordance with the provisions of 50 U.S.C. §§ 1806(f) and 1825(g).⁵

The Government expects that the Court will conclude from its *in camera*, *ex parte* review of the FISA materials that: (1) the electronic surveillance and physical searches at issue in this case were both lawfully authorized and lawfully conducted in compliance with FISA and the Fourth Amendment; (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

⁴ The Attorney General’s affidavit (“Declaration and Claim of Privilege”) is filed both publicly and attached as part of this classified filing. *See* Sealed Exhibit 1.

⁵ [CLASSIFIED MATERIAL REDACTED]

legality of the surveillance and searches without disclosing the FISA materials or portions thereof; (3) the fruits of electronic surveillance and physical searches should not be suppressed; (4) the defendant's discovery requests should be denied to the extent that they seek disclosure of FISA materials; and (5) no hearing is needed.

A. BACKGROUND

On September 20, 2012, a federal grand jury sitting in this district returned a two-count indictment charging Adel Daoud with attempted unlawful use of a weapon of mass destruction, in violation of 18 U.S.C. § 2332a(a)(2)(D), and attempted unlawful use of an explosive to damage or destroy a building used in or affecting interstate commerce, in violation of 18 U.S.C. § 844(i). (DE 16).

[CLASSIFIED MATERIAL REDACTED]

On September 18, 2012, pursuant to 50 U.S.C. §§ 1806(c) and 1825(d), the United States provided notice to Daoud 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 or physical search conducted pursuant to the Foreign Intelligence Surveillance Act of 1978 (FISA), as amended, 50 U.S.C. §§ 1801-1811, 1821-1829.” (DE 9). On August 9, 2013, Daoud filed a motion, seeking both discovery of certain “FISA-related materials” and to suppress all evidence obtained or derived from “electronic surveillance [or] any other means of collection conducted pursuant to FISA or any other foreign intelligence gathering or any intelligence agencies of the United States.” (DE 51, at 1).

[CLASSIFIED MATERIAL REDACTED]⁶

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 in detail the facts supporting the FISC's probable cause determinations with respect to the target of the electronic surveillance and physical searches and to the facilities, places, premises, or property targeted (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 requests, but also to support the United States' request, pursuant to FISA, that this Court: (1) conduct an *in camera, ex parte* review of the FISA materials; (2) find that the FISA information at issue was lawfully acquired and that the electronic surveillance and physical searches were conducted in conformity with an order of authorization or approval; and (3) order that none of the FISA materials be disclosed to the defense, and instead, that they be maintained by the United States under seal.

⁶ As a result of the redactions, the pagination and footnote numbering of the classified memorandum and the unclassified memorandum are different.

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 discussed below, a District Court also has jurisdiction to determine the legality of electronic surveillance and physical searches authorized by the FISC when the fruits of that intelligence collection are used against an “aggrieved person.”⁷ 50 U.S.C. §§ 1806(f), 1825(g).

⁷ An “aggrieved person” is defined as the target of electronic surveillance or “any other

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”).⁸ 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).

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

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). Daoud is an “aggrieved person” under FISA, and as noted above, he 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.

⁸ Pub. L. No. 107-56, 115 Stat. 272 (2001).

(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).⁹ 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).¹⁰

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.¹¹ 50 U.S.C. §§ 1804(a)(6)(B), 1823(a)(6)(B). Under FISA, "[f]oreign intelligence information" means:

⁹ [CLASSIFIED MATERIAL REDACTED]

¹⁰ 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 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).

¹¹ [CLASSIFIED MATERIAL REDACTED]

(1) information that relates to, and if concerning a United States person¹² is necessary to, the ability of the United States to protect against—

(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or

(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

(2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to —

(A) the national defense or the security of the United States; or

(B) the conduct of the foreign affairs of the United States.

50 U.S.C. § 1801(e). *See also* 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.¹³

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

¹² [CLASSIFIED MATERIAL REDACTED]

¹³ [CLASSIFIED MATERIAL REDACTED]

that each facility or place at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power;

(4) a statement of the proposed minimization procedures to be followed;

(5) a detailed description of the nature of the information sought and the type of communications or activities to be subjected to the surveillance;

(6) a certification, discussed below, of a high-ranking official;

(7) a summary of the manner or means by which the electronic surveillance will be effected and a statement whether physical entry is required to effect the electronic surveillance;

(8) the facts concerning and the action taken on all previous FISA applications involving any of the persons, facilities, or places specified in the application; and

(9) the proposed duration of the electronic surveillance.

50 U.S.C. § 1804(a)(1)-(9).

An application to conduct a physical search pursuant to FISA must contain similar information as an application to conduct electronic surveillance except that an application to conduct a physical search must also contain a statement of the facts and circumstances that justify an applicant's belief that "the premises or property to be searched contains foreign intelligence information" and that each "premises or property to be searched is or is about to be, owned, used, possessed by, or is in transit to or from" the target. 50 U.S.C. §§ 1823(a)(1)-(8), (a)(3)(B),(C).

1. The Certification

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

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

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

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

(D) designates the type of foreign intelligence information being sought according to the categories described in [50 U.S.C. §] 1801(e); and

(E) includes a statement of the basis for the certification that –

(i) the information sought is the type of foreign intelligence information designated; and

(ii) such information cannot reasonably be obtained by normal investigative techniques.

50 U.S.C. § 1804(a)(6); *see also* 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 FISA-authorized 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.¹⁴

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

¹⁴ As noted *supra*, “Attorney General” is defined in FISA as the Attorney General of the United States (or Acting Attorney General), the Deputy Attorney General, or, upon the designation of the Attorney General, the AAG/NSD. *See* 50 U.S.C. § 1801(g).

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 knowingly conspires with any person to engage in such activities;

(C) engages in international terrorism or activities in preparation therefore [sic];

(D) engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor; or

(E) engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor for or on behalf of a foreign power; or

(2) any person who –

(A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States;

(B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;

(C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power;

(D) knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power; or

(E) knowingly aids or abets any person in the conduct of activities described in [the subparagraphs above] . . . or knowingly conspires with any person to engage in activities described in [the subparagraphs above.]

50 U.S.C. §§ 1801(b)(1) and (2); *see also* 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 FISA-authorized 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 authorizing 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).

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).

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). 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. 50 U.S.C. §§ 1805(d)(2), 1824(d)(2).

III. THE DISTRICT COURT'S REVIEW OF FISC ORDERS

FISA authorizes the use in a criminal prosecution of information obtained or derived from any FISA-authorized electronic surveillance or physical search, provided that advance authorization is obtained from the Attorney General, 50 U.S.C. §§ 1806(b), 1825(c), and that proper notice is subsequently given to the court and to each aggrieved person against whom the information is to be used. 50 U.S.C. §§ 1806(c)-(d), 1825(d)-(e). 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, as Daoud has done, 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). Whether a

defendant moves to suppress FISA information under 50 U.S.C. §§ 1806(e) or 1825(f), or seeks to discover the FISA materials under some other statute or rule, the motion or request is evaluated using FISA's probable cause standard, which is discussed below, and not the probable cause standard applicable to criminal warrants. *See, e.g., United States v. El-Mezain*, 664 F.3d 467, 564 (5th Cir. 2011); *United States v. Duka*, 671 F.3d 329, 336-37 (3d Cir. 2011) (rejecting appellant's challenge to FISA's probable cause standard because it does not require any indication that a crime has been committed); *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 FISA-authorized electronic surveillance, 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.¹⁵

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

¹⁵ [CLASSIFIED MATERIAL REDACTED]

other materials relating to the surveillance [or physical search] *only where such disclosure is necessary to make an accurate determination of the legality* of the surveillance [or search].”¹⁶ 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 *El-Mezain*, 664 F.3d at 565; *United States v. Abu-Jihaad*, 630 F.3d 102, 129 (2d Cir. 2010); *United States v. Belfield*, 692 F.2d 141, 147 (D.C. Cir. 1982); *United States v. Islamic Am. Relief Agency (“IARA”)*, No. 07-00087-CR-W-NKL, 2009 WL 5169536, at *3-4 (W.D. Mo. Dec. 21, 2009); *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) (emphasis in *Nicholson*); *United States v. Kashmiri*, 2010 WL 4705159, at *2 (N.D. Ill. Nov. 10, 2010).

¹⁶ 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.

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. *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*, 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 that has addressed a motion to disclose FISA materials or to suppress FISA information has been able to reach a conclusion as to the legality of the FISA collection at issue based on its *in camera*, *ex parte* review. *See, 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 has ever 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 *United States v. Nicholson*, 955 F. Supp. 588, 592 & n. 11 (E.D. Va. 1997) (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); *United States v. Abu-Jihaad*, 531 F. Supp. 2d 299, 310 (D. Conn. 2008), *aff’d*, 630 F.3d 102, 129-30 (2d Cir. 2010); *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. Hawaii 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 Cir. 2011);¹⁷ *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 FISA-authorized electronic surveillance and physical searches that would justify this case becoming the first “exception” to the rule of all previous FISA litigation—that is, the first-ever court to order the production and disclosure of highly sensitive and classified FISA

¹⁷ All citations to *Jayyousi* herein are to the Magistrate Judge’s Report and Recommendation which was adopted and incorporated into the Court’s Opinion.

materials or the suppression of FISA-derived or -obtained evidence. Here, the FISA materials are well-organized and easily reviewable by the Court *in camera* and *ex parte*, and they are fully and facially sufficient to allow the Court to make an accurate determination that the FISA information was lawfully acquired and that the electronic surveillance and physical 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*, 531 F. Supp. 2d at 310; *Thomson*, 752 F. Supp. at 79. The Government respectfully submits that this Court, much like the aforementioned courts, is 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 now-Justice Scalia, writing for 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 counterintelligence 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”).

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. *See, e.g., El-Mezain*,

664 F.3d at 567; *Abu-Jihaad*, 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.”); *Ott*, 827 F.2d at 476-77 (FISA’s review procedures do not deprive a defendant of due process); *Gowadia*, 2009 WL 1649714, at *2; *United States v. Jayyousi*, 2007 WL 851278, at *7-8; *United States v. Benkahla*, 437 F. Supp. 2d 541, 554 (E.D. Va. 2006); *ACLU Foundation*, 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.

There remains an unbroken history of federal court holdings that FISA’s *in camera*, *ex parte* review provisions are entirely compatible with the requirements and protections of the Constitution. As stated by the United States District Court for the Northern District of Georgia, “[t]he defendants do not cite to any authority for [the proposition that FISA is unconstitutional] because there is none. Every court that has considered FISA’s constitutionality has upheld the statute from challenges under the Fourth, Fifth, and Sixth Amendments.” *United States v.*

Ahmed, No. 1:06-CR-147, 2009 U.S. Dist. LEXIS 120007, at *30 (N.D. Ga. Mar. 19, 2009) (order denying defendant's motion to disclose and suppress FISA materials).

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 such cases and that procedure is constitutional. In this case, the Attorney General has filed the required declaration invoking that procedure, and has declared that disclosure or an adversary hearing would harm national security. Accordingly, an *in camera*, *ex parte* review by this Court is the appropriate 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 of Probable Cause

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*, 630 F.3d at 130-31. *See also* 50 U.S.C. §§ 1806(f), 1825(g).

The Seventh Circuit has previously reviewed *de novo* the probable cause determination of the FISC, *United States v. Dumeisi*, 424 F.3d 526, 578 (7th Cir. 2005),¹⁸ though a minority of federal courts have afforded due deference to the findings of the FISC. *See Abu-Jihaad*, 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.”); *accord Ahmed*, 2009 U.S. Dist. LEXIS 120007, at *21-22 (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 Seventh Circuit gives deference to a magistrate judge’s probable cause determinations. *See, e.g., United States v. Robinson*, 724 F.3d 878, 884 (7th Cir. 2013) (noting the “great deference” given to the issue magistrate judge’s decision); *United States v. Carson*, 582 F.3d 827, 831 (7th Cir. 2009); *United States v. McIntire*, 516 F.3d 576, 578 (7th Cir. 2008). It would thus be consistent for a court that is reviewing FISC-authorized electronic surveillance and physical searches to adopt the same posture it would when reviewing the probable cause determination of a criminal search warrant

¹⁸ *See also 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 (explaining 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))); *Kashmiri*, 2010 WL 4705159, at *1; *Nicholson*, 2010 WL 1641167, *5. 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.

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).¹⁹

FISA requires a finding of probable cause that the target is a foreign power or an agent of a foreign power and that each facility or place at which the electronic surveillance is directed is being used, or is about to be used, or that the property or premises to be searched is, or is about 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*, 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 .

¹⁹ *Ahmed* is not alone in analogizing FISA applications to criminal search warrants. *See, e.g., 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, 742 (FISC of 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”).

. . . reflects the purpose for which FISA search orders are issued.” *Ahmed*, 2009 U.S. Dist. LEXIS 120007, at *22.

[CLASSIFIED MATERIAL REDACTED]

2. 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. at 171); *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).

3. 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 FISA-authorized 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).²⁰ 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. 2007). As the court noted:

[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 FISA-authorized electronic surveillance and physical searches at issue in this case would fall squarely within this “good faith exception.” 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

²⁰ “[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.

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]

a. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

b. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

c. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

d. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

e. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

f. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

g. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

3. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

a. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

b. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

c. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

d. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

e. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

f. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

g. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

h. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

i. **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. 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, and the standard minimization procedures ("SMPs") adopted by the Attorney General and approved by the FISC.

1. The Standard Minimization Procedures

If 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.” *Kevoork*, 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 U.S. 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 U.S. 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 Isa*, 923 F.2d 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 (S.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, we respectfully submit that the Government lawfully conducted the FISA collections discussed herein. Consequently, for the reasons stated above, the Court should find that the FISA collections discussed herein were lawfully conducted under the minimization procedures approved by the FISC and applicable to the FISA collections discussed herein.

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

In support of his motion seeking the disclosure of the FISA materials, the suppression of FISA-obtained or FISA-derived evidence, and an evidentiary hearing pursuant to *Franks v. Delaware*, 438 U.S. 154 (1978), the defendant presents numerous arguments that essentially fall into two categories: (1) that disclosure of the FISA materials is both necessary for him to litigate suppression issues, and is required by due process considerations;²¹ and (2) that the FISA-acquired evidence should be suppressed because it is unconstitutional, both on its face and as applied to him, that FISA procedural requirements were not met, probable cause was not established, and his claim that the Government relied impermissibly on activity protected by the First Amendment or captured via the FISA Amendments Act. The defendant's arguments are addressed below under these two categories.

²¹ Two distinct due process considerations are relevant. First, whether the Court's *in camera*, *ex parte* review of the challenged FISA materials under § 1806(f) accords with due process, which, as discussed above, it does. Second, whether the Court's *in camera*, *ex parte* review of the challenged FISA materials reveals information contained therein that due process requires be disclosed to the defendant, such as *Brady* material, as provided for in § 1806 (g). It is clear that the second consideration is a factual one, which the Court should defer until it conducts its *in camera*, *ex parte* review of the FISA materials.

A. THE DEFENDANT HAS NOT ESTABLISHED ANY BASIS FOR THE COURT TO DISCLOSE FISA MATERIALS TO HIM

Daoud 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). (DE 8). As noted above, every court that has addressed a motion to disclose FISA materials has denied that motion and has determined the legality of the FISA collection based on an *in camera*, *ex parte* review. The Government respectfully submits that there is nothing extraordinary about this case that would prompt this Court to be the first to order the disclosure of highly sensitive and classified FISA materials. Disclosure is simply not necessary for the Court to determine the legality of the FISA collections at issue. 50 U.S.C. §§ 1806(f) and 1825(g). Congress's clear intention is that FISA materials should be reviewed *in camera* and *ex parte*, and in a manner consistent with the realities of modern intelligence needs and investigative techniques. The Government submits that this Court is able to render a determination based on its *in camera*, *ex parte* review, and the defendant has failed to present any colorable basis for the Court to depart from that procedure.

1. Due Process Does Not Require Disclosure of the FISA Materials

Daoud claims that due process requires the disclosure of the underlying FISA applications, orders, and other materials. (DE 52, at 24-31). The Government is confident that the Court's *in camera*, *ex parte* review of the FISA materials will not reveal any material that due process requires be disclosed.

The Court's *in camera*, *ex parte* review does not violate due process, nor does due process require that the defendant be granted access to the FISA materials except as provided for in 50 U.S.C. §§ 1806(f), (g) and 1825(g). A challenge that FISA's *ex parte*, *in camera* review violates the Sixth Amendment's right to confrontation was specifically rejected in *Isa*, 923 F.2d at 1306-07, where the court ruled that the right of confrontation is "not absolute" and may bow to accommodate legitimate interests in the criminal trial process, and that, given the substantial interests at stake and the protections provided, the defendant's Sixth Amendment rights were not violated. Similar Sixth Amendment arguments were advanced unsuccessfully in *Warsame* 547 F. Supp. 2d at 988 n.4 (citing to *Nicholson*, 955 F. Supp. at 592); *Belfield*, 692 F.2d at 148; *Megahey*, 553 F. Supp. at 1193; *Benkahla*, 437 F. Supp. 2d at 554; *Nicholson*, 955 F. Supp. at 592 & n.11; *United States v. Falvey*, 540 F. Supp. 1306, 1315-16 (E.D.N.Y. 1982) (rejecting challenges under the First, Fifth, and Sixth Amendments). As summarized by the United States District Court for the Northern District of Georgia, "[t]he defendants do not cite to any authority for [the proposition that FISA is unconstitutional] because there is none. Every court that has considered FISA's constitutionality has upheld the statute from challenges under the Fourth, Fifth, and Sixth Amendments." *Ahmed*, No. 1:06-CR-147, 2009 U.S. Dist. Lexis 120007, at *30.

As previously noted, the necessity of disclosing FISA materials is a factual, not legal, question.²² With respect to any claim that the FISA materials contain information that due process requires be disclosed to the defense, such request is premature since the Court will make that factual determination for itself during its *ex parte, in camera* review. The Government submits that the Court will determine after its *ex parte, in camera* review of the FISA materials that they do not contain any discoverable material that has not been provided to the defense, but which due process mandates be disclosed. The Court should therefore decline to disclose the FISA materials on the asserted due process grounds. With respect to the defense claim that due process requires that it should be involved in the Court's *ex parte, in camera* review, the consistent rulings of federal courts have held to the contrary and are dispositive on this issue.

2. *Franks v. Delaware* Does Not Require Disclosure of FISA Materials

Daoud also speculates that there may have been significant omissions or reckless statements in the applications submitted to the FISC, in violation of *Franks v. Delaware*, 438 U.S. 154 (1978). He therefore seeks the disclosure of the FISA materials so they can attempt to provide a basis for their speculation. (DE 52, at 25). This is an admission by the defendant that he has no articulable support for his request for a *Franks* hearing. In fact, the legal prerequisite for such a hearing is

²² “If the court determines that the surveillance was lawfully authorized and conducted, it shall deny the motion of the aggrieved person except to the extent that due process requires discovery or disclosure.” 50 U.S.C. §§ 1806 (g) and 1825(h).

that 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.

Daoud, however, stands this principle on its head and offers the unsupported assertion that *Franks* compels disclosure. (DE 52, at 21).²³ Under this theory, Daoud or a similarly situated defendant need only allege some *Franks* impropriety, without more, to obtain the FISA applications and related materials. That argument disregards both the clear language of 50 U.S.C. §§ 1806(f) and 1825(g) (that the Court may disclose FISA material to the defense *only* when it is unable to determine the lawfulness of the surveillance based on its own *in camera*, *ex parte* review) and the requirements set out in *Franks* for a hearing, which places the onus squarely on the moving party.

To merit an evidentiary hearing under *Franks*, a defendant must first make a “concrete and substantial preliminary showing” that: (1) the affiant deliberately or recklessly included false statements, or failed to include material information, in the affidavit; and (2) the misrepresentation was essential to the finding of probable cause. *Franks*, 438 U.S. at 155-56; *United States v. Colkley*, 899 F.2d 297, 301 (4th Cir. 1990); *Kashmiri*, 2010 WL 4705159, at * 6 (defendant “has not made any showing—let alone a substantial one—that an Executive Branch officer knowingly

²³ [CLASSIFIED MATERIAL REDACTED]

and intentionally, or recklessly, included a false statement in the FISA application [and w]ithout such a showing, he is foreclosed from obtaining a hearing”); *Duggan*, 743 F.2d at 77 n.6. Failure of the defendant “to satisfy either of these two prongs proves fatal to a *Franks* hearing.” *Kashmiri*, 2010 WL 4705159, at * 5; *Mubayyid*, 521 F. Supp. 2d at 130-31.

The defendant’s burden in establishing the need for a *Franks* hearing is a heavy one. *United States v. Jeffus*, 22 F.3d 554, 558 (4th Cir. 1994). A defendant’s “attack must be more than conclusory and must be supported by more than a mere desire to cross-examine.” *Franks*, 438 U.S. at 171; *Kashmiri*, 2010 WL 4705159, at * 6 (“Without producing the requisite offer of proof of impropriety in the FISA application, however, this argument is merely conclusory, and equates to an improper indirect attack on the FISA procedures”). A defendant must submit allegations of deliberate falsehood or of reckless disregard for the truth, accompanied by an offer of proof. *Franks*, 438 U.S. at 171. 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.” *Colkley*, 899 F.2d at 301-02. If a defendant could force disclosure of FISA materials and obtain an adversary hearing merely by speculating that there *might* be information somewhere in an application that could possibly provide grounds for a *Franks* hearing, the disclosure of FISA materials and adversary hearings would become the rule and not the unprecedented exception. Such a result would violate Congress’ clear intention that the FISA

materials should be reviewed *in camera* and *ex parte*, and in a manner consistent with the realities of modern intelligence needs and investigative techniques.

Only after a defendant makes the requisite showing²⁴ may the Court conduct a *Franks* hearing to determine if there are material 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. Here, Daoud has not made the requisite showing but has instead claimed that they require the disclosure of the FISA materials to attempt to make that showing. The FISA statute does not, however, envision such disclosure without establishing a basis for it. “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.

²⁴ Indeed, even if a defendant offers sufficient proof to show that an affidavit involved false statements or omissions, a hearing should not be held if 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).

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

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").

The defendant has failed to carry his burden of establishing the prerequisites for a *Franks* hearing. Furthermore, the attempt to obtain disclosure of the FISA materials so that he might attempt 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 Court should therefore decline to disclose the FISA materials on the basis asserted by the defense, and should deny the defendant's request for a *Franks* hearing or disclosures based on *Franks*.

3. Daoud's Age Does Not Necessitate Disclosure

The defendant also claims that "[t]o the extent that FISA activity pre-dated September 21, 2011, when Defendant turned eighteen years old," this Court should order the disclosure of FISA applications and warrants. (DE 52, at 18). The defendant's arguments include an unexplained reference to *parens patriae* and a similarly unexplained claim that the defendant's age is "relevant to the government's action under FISA and the Fourth Amendment." (DE 52, at 18). Daoud, however, was never in the care of the federal government or in any other

relationship with the state that would trigger some special consideration. Contrary to the defendant's claim, no portion of FISA makes an aggrieved person's age relevant.

[CLASSIFIED MATERIAL REDACTED]

4. There Is No Basis for Disclosure Related to the FISA Amendments Act of 2008

Like other prior motions from the defendant, Daoud seeks additional disclosures related to any surveillance conducted pursuant to Section 702 of the FISA Amendments Act of 2008 ("FAA"). Pub. L. 110-261, § 702, 122 Stat. 2436, 2438-48 (2008). Daoud asks this Court to "examine whether any portion of the FISA was requested and conducted pursuant to the authority provided in [Section 702] . . . or whether any information in the FISA applications was the product of surveillance authorized under the FAA." (DE 52, at 15). Daoud also seeks FAA-related disclosures and discovery from the Government, asking the Court to "compel the government to disclose whether any such information [that it intends to use at trial] was the product of . . . or of such surveillance authorized pursuant to the FAA." (DE 52, at 16). Daoud also asks the Government to disclose "the nature of the FAA surveillance in this case even if, for instance[,] Defendant's communications themselves were not intercepted." (DE 52, at 15 n.11).

Any discovery based on the FAA is unwarranted here because the FAA is simply not at issue in this case. As the Government explained in a previous filing, it "does not intend to use any such evidence obtained or derived from FAA-authorized

surveillance in the course of this prosecution.” (DE 49, at 2). Upon this representation by the Government, this Court should deny the defendant’s new motion for discovery and disclosure based on the FAA.²⁵ Similarly, because the Government does not intend to offer any evidence obtained or derived from FAA surveillance, the defendant’s motion to suppress such evidence should be denied.

[CLASSIFIED MATERIAL REDACTED]

B. THE DEFENDANT HAS NOT ESTABLISHED ANY BASIS FOR THE COURT TO SUPPRESS THE FISA-ACQUIRED EVIDENCE

The defendant’s motion presents a laundry list of objections to the relevant FISA collection, ranging from claims that the applications failed to establish the requisite probable cause under FISA to allegations that the applications were based on unreliable or impermissible sources of information. These arguments are without merit, and the Government will respond to each category below.

1. The Government Satisfied the Probable Cause Requirements under FISA

First, Daoud claims that the FISA applications failed to establish probable cause that Daoud was an agent of a foreign power. (DE 52, at 2, 11-13). The crux of

²⁵ The defendant’s claim that the Government should disclose “the nature of the FAA surveillance in this case even, for instance[,] Defendant’s communications themselves were not intercepted” is perplexing. (DE 52, at 15 n.11). If Daoud’s communications were not intercepted, or his facilities not targeted, he would not be aggrieved and have no basis to challenge the collection. The Government sees no legal relevance to his broad discovery request.

Moreover, the defendant has also made multiple claims, in this motion and others, based on his interpretation of a single public remark. While the Government appreciates the defendant’s position in litigating FISA-related matters, it offers that the defendant may misunderstand this public remark, which is not a revelation that has any legal implication.

Daoud's claim is that a "high school student from suburban Chicago" could not possibly be an agent of a foreign power. As an initial matter, the defendant offers a naïve understanding of the level of criminality in which individuals of his age can engage in.

[CLASSIFIED MATERIAL REDACTED]

a. [CLASSIFIED MATERIAL REDACTED]

[CLASSIFIED MATERIAL REDACTED]

b. "Raw Intelligence" Is Not Inherently Unreliable

The defendant argues that the FISA applications are flawed because they may include what he calls "raw intelligence." (DE 52, at 13). Although he does not define "raw intelligence," some case law has used the term. For example, in *Bensayah v. Obama*, the court discussed "raw intelligence" in the context of an intelligence report that contained the warning 'INFORMATION REPORT, NOT FINALLY EVALUATED INTELLIGENCE.'²⁶ 610 F.3d 718, 725 (D.C. Cir. 2010).

As courts have noted, however, there is thus nothing inherently unreliable about "raw intelligence," which may either contain sufficient indicia of reliability within its four corners, or if not, may be relied upon if it is appropriately corroborated. *Parhat v. Gates*, 532 F.3d 834, 847, 849 (D.C. Cir. 2008); *see also Bensayah*, 610 F.3d at 725-26. In *Khan v. Obama*, for example, the district court concluded that "raw intelligence" was "reliable." *Khan v. Obama*, 741 F. Supp. 2d 1, 6, 12-15 (D.D.C. 2010). The D.C. Circuit Court upheld the district court's

²⁶ [CLASSIFIED MATERIAL REDACTED]

conclusions about the reliability of that intelligence, offering a detailed discussion about the intrinsic and extrinsic indicia of “raw intelligence” reliability. *Khan v. Obama*, 655 F.3d 20, 26-31 (D.C. Cir. 2011).

This Court should decline to suppress the FISA-acquired evidence regardless whether any “raw intelligence” information was presented to the FISC. No court has held that such information is inherently unreliable, and in fact the case law makes clear “that ‘raw’ intelligence is not inherently unreliable.” *Alsabri v. Obama*, 764 F. Supp. 2d 60, 91 (D.D.C. 2011).

2. There Is No Basis for Suppression Related to the FISA Amendments Act of 2008

Daoud also moves to suppress the evidence obtained or derived from FISA, on the alleged basis that “any part of the FISA surveillance . . . conducted pursuant to the FAA” violates “several Fourth Amendment principles,” the First Amendment, and Article III of the Constitution’s separation of powers principle. (DE 52, at 15-16). The Government’s response to such claims has already been discussed *supra* with regard to the defendant’s disclosure motions based on FAA-related claims, and for sake of brevity it will not repeat those arguments here.

[CLASSIFIED MATERIAL REDACTED]

3. The FISA Surveillance in Question Was Not Conducted Solely on Daoud’s Protected First Amendment Activity

Daoud also questions “whether there was any basis, *other than protected First Amendment activity*, for commencing FISA surveillance on Defendant,” (DE 52, at 17), speculating that FISA surveillance was predicated on his expression of

opinions online. Daoud is of course correct that FISA prohibits the targeting of a U.S. person based *solely* on First Amendment protected activities. 50 U.S.C. §§ 1805(a)(2)(A), 1824(a)(2)(A). As various courts have explained however, this rule does not prohibit any consideration of statements by a target and 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).

[CLASSIFIED MATERIAL REDACTED]

4. **A Significant Purpose of the FISA Surveillance Was the Collection of Foreign Intelligence Information**

Daoud also claims that “any foreign intelligence that could possibly be gleaned [from FISA surveillance] could not possibly serve as a significant purpose of FISA surveillance.” (DE 52, at 21-22). The defense again emphasizes the age of the defendant as evidence that foreign intelligence information could not possibly have been a significant purpose. As noted earlier, however, neither the statute nor our national experience suggests there is a minimum age requirement for terrorism-related activities.

[CLASSIFIED MATERIAL REDACTED]

C. **FISA’S SIGNIFICANT PURPOSE STANDARD COMPLIES WITH THE REQUIREMENTS OF THE FOURTH AMENDMENT**

In his final salvo, Daoud argues that this Court should find FISA’s “significant purpose” standard unconstitutional in light of the “recent widely

publicized public disclosures regarding the expansive nature of the NSA PRISM program and the like—particularly insofar as they involve the collection of domestic communications of American citizens.” (DE 52, at 33). First, this argument conflates different FISA programs—“traditional FISA” with FAA surveillance and Section 215 of FISA surveillance. As the Government has explained, this case singularly involves “traditional” FISA surveillance. Second, as Daoud concedes, “courts have found that the reduced ‘significant purpose’ standard does not violate the Constitution.” (DE 52, at 33).

In 2001, FISA was amended by the USA PATRIOT Act which, *inter alia*, required that an Executive Branch official now certify that “a significant purpose” of the requested surveillance was to obtain foreign intelligence information. 50 U.S.C. § 1804(a)(6)(B). The defendant has challenged the constitutionality of the significant-purpose test based on a misunderstanding of the rationale underlying the superseded primary-purpose test. As the Third Circuit observed in *Duka*, “the dispositive issue is whether the ‘significant purpose’ test is reasonable. . . . We agree with our sister courts of appeals and the Foreign Intelligence Surveillance Court of Review that the amended FISA’s ‘significant purpose’ standard is reasonable under the Fourth Amendment.” 671 F.3d at 343. The Government submits that this Court’s *in camera* and *ex parte* review of the FISA materials will reveal ample evidence that a significant purpose of the challenged surveillance was to obtain foreign intelligence information.

The primary-purpose test was derived from a consideration of *warrantless* searches that were conducted pursuant to the Executive's Article II foreign affairs powers prior to the enactment of FISA, and without any prior judicial involvement. *See, e.g., Abu Jihaad*, 630 F.3d at 121. In that context, warrantless surveillance was conducted by the Government as an exception to the Fourth Amendment, and was therefore limited by the scope of the Constitution's grant of authority to the Executive to conduct foreign affairs. *United States v. Truong Dinh Hung*, 629 F.2d 908, 912-16 (4th Cir. 1980).²⁷ Several courts imported that primary purpose test from the warrantless surveillance context into their statutory interpretation of FISA's certification requirement. *See Duggan*, 743 F.2d at 77; *Pelton*, 835 F.2d at 1075-76; *Badia*, 827 F.2d at 1464; *United States v. Johnson*, 952 F.2d 565, 572 (1st Cir. 1991). Contrary to the defendant's assertions, however, none of those cases held that the primary purpose test was constitutionally mandated. For example, the Second Circuit has explicitly stated that "in *Duggan*, we construed FISA's original reference to electronic surveillance for 'the purpose' of obtaining foreign intelligence

²⁷ In *Truong*, the Fourth Circuit was presented with wholly warrantless surveillance, carried out by the Executive Branch unilaterally and without any judicial involvement whatsoever. The Court crafted the "primary purpose" test to identify the circumstances in which the Executive Branch may constitutionally dispense with judicial oversight altogether. This case, in contrast, involves the constitutional prerequisites for surveillance conducted pursuant to the detailed statutory scheme created by FISA, with its elaborate sets of procedures and rules that subject foreign intelligence surveillance to judicial oversight and approval. There is nothing in *Truong's* reasoning to suggest that the judicially safeguarded FISA process requires the alternative safeguard of a "primary purpose" limitation that was found to be appropriate when the judiciary was completely excluded from the process.

information, as a ‘requirement that foreign intelligence information be the *primary* objective . . . we were identifying Congress’s intent in enacting FISA, not a constitutional mandate. . . . In short, nothing in *Duggan* erected a constitutional bar to Congress reconsidering and reframing the purpose requirement of FISA.” *Abu Jihad*, 630 F.3d at 123.

The pre-USA PATRIOT Act FISA language required that the Government certify that “the purpose” of the surveillance was the acquisition of foreign intelligence information. By interpreting “the purpose” to mean “the primary purpose”—and not to mean the sole purpose—the various courts provided that an additional purpose could be something other than the acquisition of foreign intelligence information, such as criminal investigation and prosecution. The defendant’s reliance on *United States v. Johnson* is misplaced because while the Court in *Johnson* clearly stated that “the investigation of criminal activity cannot be the primary purpose of the surveillance,” it did not say that it cannot be a purpose of the surveillance. Further, the Ninth Circuit specifically refused to define FISA’s original “purpose” requirement and upheld a district court’s refusal to suppress evidence derived from FISA surveillance. In *United States v. Sarkissian*, 841 F.2d 959, 965 (9th Cir. 1988), the Court refused “to draw too fine a distinction between criminal and intelligence investigations,” because by definition international terrorism requires the investigation of some activities that also constitute crimes, and “FISA contemplates prosecution based on evidence gathered through surveillance.”

Since the primary purpose test was the result of statutory construction, and was not a reflection of constitutional necessity, the abrogation of that language by the USA PATRIOT Act cannot, and does not, create a constitutional issue.

With the exception of the now-vacated and legally null *Mayfield v. United States*, 504 F. Supp. 2d 1023 (D. Or. 2007), *vacated*, 599 F.3d 964 (9th Cir. 2010)²⁸ every court that has considered the significant-purpose test has held that test to be constitutional. *See Abu Jihaad*, 630 F.3d at 128 (“[w]e conclude simply that FISA’s ‘significant purpose’ requirement . . . is sufficient to ensure that the executive may only use FISA to obtain a warrant when it is in good faith pursuing foreign intelligence gathering [and the] fact that the government may also be pursuing other purposes, including gathering evidence for criminal prosecution, compels no different conclusion”); *Ning Wen*, 477 F.3d at 897; *In re Sealed Case*, 310 F.3d at 746; *Warsame*, 547 F. Supp. 2d at 992-97; *Mubayyid*, 521 F. Supp. 2d at 139; *United States v. Marzook*, 435 F. Supp. 2d 778, 786 (N.D. Ill. 2006); *Benkahla*, 437 F. Supp. 2d at 554; *Jayyousi*, 2007 WL 851278, at *1. In fact, in *In re Sealed Case*, the Court noted that *Truong*’s reliance on the “primary purpose” test was misconceived because it was based on the false “assertion that once the government moves to

²⁸ FISA’s “significant purpose” standard was held unconstitutional in a civil case, which no other court followed and which the Ninth Circuit eventually vacated on the ground that the plaintiff lacked standing. *See Mayfield v. United States*, 599 F.3d 964 (9th Cir. 2010). And, as is the case for the lower court’s decision in *Mayfield*, when a judgment is vacated by a higher court “it deprives the [lower] court’s opinion of precedential effect.” *Los Angeles Cnty. v. Davis*, 440 U.S. 625, 634 n. 6 (1979). Moreover, the district court’s rationale in *Mayfield* was specifically rejected in *Kashmiri*, 2010 U.S. Dist. LEXIS 119470, at *8. It is that rejected rationale, from a legally null opinion, that Daoud urges this Court to adopt.

criminal prosecution its ‘foreign policy concerns recede’. . . . [But] the government’s primary purpose is to halt the espionage or terrorism efforts.” *In re Sealed Case*, 310 F.3d at 743. To accomplish that objective, “arresting and prosecuting terrorist agents of, or spies for, a foreign power may well be the best technique to prevent them from successfully continuing their terrorist activities.” *Id.* at 724. In short, resort to criminal prosecution does not mean that the Government’s foreign policy and national security concerns have fallen out of the equation; it simply means that the Government has chosen prosecution as one means of pursuing those concerns.

As the Third Circuit noted in *Duka*, the “significant purpose” standard “reflects a balance struck by Congress . . . to promote coordination between intelligence and law enforcement officials in combating terrorism, acknowledging that, as a practical matter, these functions inevitably overlap.” 671 F.3d at 329. The Court noted that *Keith*, 407 U.S. at 322-23, required that Congress’s judgment should on this issue be accorded “some additional measure of deference” by the courts, and added that “even leaving Congress’s judgment aside, we conclude that FISA’s “significant purpose” standard is reasonable in light of the government’s legitimate national security goals.” *Id.* As the *Sherifi* court observed, “Congress safeguarded against the possibility of obtaining FISA warrants without a good faith purpose to obtain foreign intelligence information by demanding that in every FISA application a certification that a ‘significant purpose’ of the surveillance or search is to obtain foreign intelligence information.” *Sherifi*, 793 F. Supp. 2d at 758-59.

VI. CONCLUSION

The defendant's motion should be denied. Courts have uniformly held that the probable cause requirement of FISA comports with the requirements of the Fourth Amendment to the United States Constitution (*see, e.g., Isa*, 923 F.2d at 1304), and that 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); *United States v. Damrah*, 412 F.3d 618, 624 (6th Cir. 2005); *Warsame*, 547 F. Supp. 2d at 988-89. Daoud advances no argument to justify any deviation from these well-established precedents.

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

Even if this Court were to determine that the acquisition of the FISA information had not been lawfully acquired or that the electronic surveillance and physical searches were not made in conformity with an order of authorization or approved, the FISA evidence would nevertheless be admissible under the "good faith" exception to the exclusionary rule articulated in *United States v. Leon*, 468 U.S. 897 (1984). *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.

The Attorney General has filed a declaration in this case stating that disclosure 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 finds that disclosure is necessary to the Court’s accurate determination of the legality of the FISA collection.

The Government respectfully submits that the Court can make this determination without disclosing the classified and highly sensitive FISA materials to the defendant. Every federal court that has been asked to determine the legality of a FISA-authorized collection has been able to do so *in camera*, *ex parte* and without the assistance of defense counsel. 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.

Based on the foregoing analysis, the Government respectfully submits that the Court should: (1) conduct an *in camera*, *ex parte* review of the FISA materials and the Government's classified submission; (2) find that the electronic surveillance and physical searches at issue in this case were both lawfully authorized and lawfully conducted in compliance with the Fourth Amendment; (3) hold that disclosure of the FISA materials and the Government's classified submissions to the defendant is not authorized because the Court is able to make an accurate determination of the legality of the surveillance without disclosing the FISA materials or any portions thereof; (4) hold that the fruits of electronic surveillance, physical searches, or both, should not be suppressed; (5) 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 (6) deny the defendant's motion without an evidentiary hearing.²⁹

²⁹ A district court order granting motions or requests under 50 U.S.C. § 1806(g), a decision that electronic surveillance was 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). 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

DATED: October 25, 2013

Respectfully submitted,

ZACHARY T. FARDON
United States Attorney

s/William E. Ridgway
WILLIAM E. RIDGWAY
BARRY JONAS
Assistant United States Attorneys

s/Bridget Behling
BRIDGET BEHLING
Trial Attorney
Counterterrorism Section
National Security Division, Department of Justice

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.

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

CASE NO. 12-CR-723

UNITED STATES OF AMERICA,)	
)	
Plaintiff)	DECLARATION AND CLAIM
)	OF PRIVILEGE
v.)	
)	
ADEL DAOUD,)	
)	
Defendant.)	

DECLARATION AND CLAIM OF PRIVILEGE
OF THE ATTORNEY GENERAL OF THE UNITED STATES

I, Eric H. Holder, Jr., hereby declare the following:

1. I am the Attorney General of the United States of America and head of the United States Department of Justice, an Executive Department of the United States. I have official custody of and control over the files and records of the United States Department of Justice. The matters stated herein are based on my knowledge, on consideration of information available to me in my official capacity as Attorney General, on discussions that I have had with other Department of Justice officials, and on conclusions I have reached after my review of this information.

2. Under the authority of 50 U.S.C. §§ 1806(f) and 1825(g), I submit this declaration pursuant to the Foreign Intelligence Surveillance Act of 1978 ("FISA"), as amended, in connection with the above-captioned criminal proceeding. I have been advised that the Government presently intends to use information obtained or derived from FISA-authorized electronic surveillance and physical searches in the criminal proceeding against the Defendant.

See 50 U.S.C. §§ 1806(c) and 1825(d). Accordingly, Defendant Adel Daoud, by and through his attorneys, has filed a motion seeking disclosure and suppression of FISA-related materials (hereinafter collectively the "Defendant's Motion"). The Government will file an opposition to the Defendant's Motion. For the reasons set forth in the Government's Opposition, it is necessary to provide this Court with the applications submitted to, and the orders issued by, the Foreign Intelligence Surveillance Court ("FISC"), as well as other related documents (hereinafter collectively referred to as "the FISA Materials").

3. Based on the facts and considerations set forth below, I hereby claim that it would harm the national security of the United States to disclose or to hold an adversarial hearing with respect to the FISA Materials. The United States will be submitting the relevant classified documents to this Court as part of a "Sealed Appendix," so that this Court may conduct an *in camera, ex parte* review of the legality of the FISA collection at issue. My Claim of Privilege also extends to the classified portions of any memoranda and briefs the Government may file in connection with this litigation and to any oral representations that may be made by the Government that reference the classified information contained in the FISA Materials.

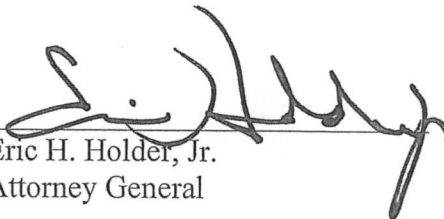
4. In support of my Claim of Privilege, the United States is submitting to the Court for *in camera, ex parte* review the Declaration of R.J. Holley, Acting Assistant Director, Counterterrorism Division, Federal Bureau of Investigation. Mr. Holley's Declaration sets forth, in detail, the specific facts on which my Claim of Privilege is based. The Declaration of Mr. Holley is classified at the "TOP SECRET" level.

5. Relying on the facts set forth in Acting Assistant Director Holley's Declaration, I certify that the unauthorized disclosure of the FISA Materials that are classified at the "TOP SECRET" level could reasonably be expected to cause exceptionally grave damage to the

national security of the United States. I further certify that the unauthorized disclosure of the FISA materials that are classified at the "SECRET" level reasonably could be expected to cause serious damage to the national security of the United States. The FISA Materials contain sensitive and classified information concerning United States intelligence sources and methods and other information related to efforts of the United States to conduct counterterrorism investigations, including the manner and means by which those investigations are conducted. As a result, the unauthorized disclosure of that information could harm the national security interests of the United States.

6. I respectfully request that the Court treat the contents of the Sealed Appendix, for security purposes, in the same sensitive manner that the contents were treated in the submission to this Court, and to return the Sealed Appendix to the Department of Justice upon the disposition of the Defendant's Motion. The Department of Justice will retain the Sealed Appendix under the seal of the Court subject to any further orders of this Court or other courts of competent jurisdiction.

Pursuant to Title 28, United States Code, Section 1746, I declare under penalty of perjury that the foregoing is true and correct. Executed on October 16, 2013.


Eric H. Holder, Jr.
Attorney General