

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION**

UNITED STATES OF AMERICA

v.

ASHRAF AL-SAFOO

Case No. 18-CR-696

Judge John Robert Blakey

MEMORANDUM OPINION AND ORDER

On October 17, 2018, the Federal Bureau of Investigation arrested Defendant Al-Safoo pursuant to a criminal complaint charging him with conspiracy to provide material support to a designated foreign terrorist organization, in violation of 18 U.S.C. § 2339B. [1].

On October 23, 2018, pursuant to 50 U.S.C. §§ 1806(c) and 1825(d), the Government provided notice to Defendant and this Court that it “intends to offer into evidence, or otherwise use or disclose in any proceedings in this matter, information obtained and derived from electronic surveillance and physical search conducted pursuant to the Foreign Intelligence Surveillance Act.” [10].

On March 12, 2020, a grand jury in the Northern District of Illinois returned a second superseding indictment charging the defendant with five counts of providing material support to the Islamic State of Iraq and ash-Sham (“ISIS”), in violation of 18 U.S.C. § 2339B(a)(1); one count of conspiracy to provide material support to ISIS, in violation of 18 U.S.C. § 2339B(a)(1); four counts of intentionally accessing a computer without authorization, in violation of 18 U.S.C. §§ 1030(a)(2)(C) and 1030(c)(2)(B)(ii); one count of conspiracy to intentionally access a computer without authorization, in violation of 18 U.S.C. §§ 371, 1030(a)(2), and 1030(c)(2)(B)(iii); and

one count of conspiracy to transmit threats in interstate commerce, in violation of 18 U.S.C. §§ 371 and 875(c). [162].

On December 11, 2020, Defendant moved for disclosure of FISA-related materials, production of discovery relating to FISA-surveillance, and for suppression of evidence obtained or derived from FISA-authorized surveillance [222] and [223].

On April 2, 2021, the government filed a response in opposition to Defendant's Motions. [274].

On March 23, 2021, Defendant filed his consolidated reply. [282].

I. Findings

Under the Foreign Intelligence Surveillance Act (FISA), the law contains specific and detailed procedures required for obtaining orders to authorize electronic surveillance and physical search of a foreign power or an agent of a foreign power. To begin the FISA process, an application approved by the Attorney General that contains specific information is filed *ex parte* and under seal with the Foreign Intelligence Surveillance Court (FISC). 50 U.S.C. §§ 1804(a), 1823(a). The FISC must make necessary, specific findings after reviewing an application before entering an *ex parte* order, 50 U.S.C. §§ 1805(a), 1823(a), which specifically identifies the targeted facilities and directs how the electronic surveillance and physical search are to be conducted. 50 U.S.C. §§ 1805(c)(1)-(2), 1824(c)(1)-(2).

The Court has reviewed Defendant's Motions and the government's response and the Sealed Appendix thereto, including the FISA materials, and Defendant's reply *in camera* and *ex parte*, and based upon its analysis of all the materials submitted to the Court, finds that:

(1) The President has authorized the United States Attorney General to approve applications to the FISC for electronic surveillance and for physical search for foreign intelligence information and purposes;

(2) Each application was made by a federal officer and approved by the Attorney General (50 U.S.C. §§ 1805(a)(1), 1824(a)(1));

(3) Each application contained facts establishing probable cause to believe that the target of the electronic surveillance, physical search, or both, was at the time an agent of a foreign power (50 U.S.C. §§ 1801(b)(2), 1805(a)(2)(A), 1824(a)(2)(A));

(4) No United States person was determined to be an agent of a foreign power solely upon the basis of activities protected by the First Amendment to the United States Constitution (50 U.S.C. §§ 1805(a)(2)(A), 1824(a)(2)(A));

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

(6) Each application made pursuant to 50 U.S.C. § 1823 contained facts establishing probable cause to believe that the premises or property to be searched was or was about to be owned, used, possessed by, or was in transit to or from, an agent of a foreign power or a foreign power (50 U.S.C. § 1824(a)(2)(B));

(7) Each application made pursuant to 50 U.S.C. § 1823 contained facts establishing probable cause to believe that the premises or property to be searched contained foreign intelligence information (50 U.S.C. §§ 1823(a)(3)(B), 1824(a)(4));

(8) The minimization procedures incorporated into the application(s) and order(s) met the requirements of 50 U.S.C. §§ 1801(h) or 1821(4) (50 U.S.C. §§ 1805(a)(3), 1824(a)(3)), and the government implemented such minimization procedures in conformity with an order of authorization or approval;

(9) Each application contained all of the statements and certifications required by 50 U.S.C. §§ 1804 or 1823 (50 U.S.C. §§ 1805(a)(4), 1824(a)(4));

(10) No certification in an application for a target who was at the time a United States person was clearly erroneous on the basis of the statement made pursuant to 50 U.S.C. §§ 1804(a)(6)(E) or 1823(a)(6)(E) or any other information furnished under 50 U.S.C. §§ 1804(c) or 1823(c) (50 U.S.C. §§ 1805(a)(4), 1824(a)(4));

(11) A “significant purpose” of the government’s collection pursuant to FISA was to collect foreign intelligence information (50 U.S.C. §§ 1804(a)(6)(B), 1823(a)(6)(B));

(12) Each order issued by the FISC satisfied the requirements of 50 U.S.C. §§ 1805(c) or 1824(c);

(13) Each order issued by the FISC satisfied the requirements of 50 U.S.C. §§ 1805(d) or 1824(d);

(14) The defendant made no preliminary or substantial showing of a false statement, nor of a false statement that was material, nor a statement that was made knowing or intending it was false or with reckless disregard for its truth, in the FISA application(s) that would entitle him to a hearing pursuant to *Franks v. Delaware*, 438 U.S. 154 (1978). As there is no indication of any such false statements in the FISA application(s), a *Franks* hearing is not warranted in this matter;

(15) Disclosure to the defense of the FISA materials is not required because the Court was able to make an accurate determination of the legality of the electronic surveillance and physical search without disclosing the FISA materials or any portions thereof;

(16) Due process does not otherwise require disclosure of the FISA materials; and

(17) The government complied with its notice obligations under FISA, and any additional notice regarding any surveillance techniques used, the legal authorities relied upon, or any underlying warrants, orders, or applications used in connection with such surveillance is not merited.

II. Discussion

The defendant seeks materials that were presented to the FISC, including the resulting FISC order(s), that provided the legal basis for the electronic surveillance and physical search from which some of the evidence that will be used against him was obtained or derived. By requesting the disclosure of the FISA materials, the defendant is seeking discovery of material that FISA specifically protects from such disclosure, except as provided in 50 U.S.C. §§ 1806(f), (g) and 1825(g), (h) (*i.e.*, if disclosure is necessary for the Court to make a determination of the legality of the surveillance or search, or if due process requires discovery or disclosure).¹

¹ Two distinct due process considerations governed this Court's consideration. First, this Court considered whether the *in camera*, *ex parte* review process mandated by 50 U.S.C. §§ 1806(f) and 1825(g) accorded with due process. Consistent with cited authority, it does. Second, this Court considered whether the FISA materials contain any information that due process requires be disclosed to the defendant (*e.g.*, *Brady* material) under 50 U.S.C. §§ 1806(g) and 1825(h). They do not.

In this case, the Attorney General has filed a sworn declaration stating that disclosure of the FISA materials or an adversary hearing would harm the national security of the United States. Therefore, as mandated by FISA, this Court conducted an *in camera*, *ex parte* review of the FISA materials to determine whether the information was lawfully acquired and whether the electronic surveillance and physical search were made in conformity with an order of authorization or approval (*i.e.*, were lawfully conducted). This *in camera*, *ex parte* review process under FISA satisfies due process under the United States Constitution. *See, e.g., United States v. Daoud*, 755 F.3d 479, 482–83 (7th Cir. 2014); *United States v. El-Mezain*, 664 F.3d 467, 567 (5th Cir. 2011); *United States v. Abu-Jihaad*, 630 F.3d 102, 117 (2d Cir. 2010); *United States v. Damrah*, 412 F.3d 618, 624 (6th Cir. 2005); *United States v. Ott*, 827 F.2d 473, 476–77 (9th Cir. 1987) (ruling FISA’s *in camera*, *ex parte* procedures do not deprive a defendant of due process); *United States v. Butenko*, 494 F.2d 593, 607 (3d Cir. 1974); *United States v. Warsame*, 547 F. Supp. 2d 982, 988–89 (D. Minn. 2008); *United States v. Spanjol*, 720 F. Supp. 55, 58–59 (E.D. Pa. 1989). 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).

After conducting its own review of the FISA materials, the Court finds that it does not require the assistance of the defense to make an accurate determination of the legality of the electronic surveillance and physical search. Thus, there is no valid, legal reason for disclosure of any of the FISA materials to the defendant. *See Daoud*, 755 F.3d at 485 (because the district court was capable of making the determination

of legality on its own, holding that disclosure was “not ‘necessary’ under any definition of that word”); *United States v. Duggan*, 743 F.2d 59, 78 (2d Cir. 1984) (holding that disclosure should occur only if the court determines that such disclosure is necessary to make an accurate determination of the legality of the surveillance).

As a result of the Court’s thorough *in camera*, *ex parte* examination of the materials in the Sealed Appendix, the Court finds that the FISA materials provide all of the information needed to address Defendant’s Motions. The Court finds that the government satisfied FISA’s requirements to obtain orders for electronic surveillance and physical search; that the information obtained pursuant to FISA was lawfully acquired; and that the electronic surveillance and physical search were made in conformity with an order of authorization or approval.

Additionally, there is no basis for disclosure of the FISA materials pursuant to 50 U.S.C. §§ 1806(g) and 1825(h). Such disclosure is only permitted if this Court’s *in camera*, *ex parte* review revealed that due process requires discovery or disclosure. The Court finds that due process does not require disclosure of the FISA materials to the defendant.

Although federal courts disagree about whether the FISC’s probable cause determinations should be reviewed *de novo* or accorded deference, the Court finds that the materials that it has reviewed *in camera*, *ex parte* satisfy either standard. The Court also finds that the probable cause requirement of FISA comports with the requirements of the Fourth Amendment to the United States Constitution. *See, e.g., United States v. Ning Wen*, 477 F.3d 896, 898 (7th Cir. 2007) (holding that FISA is constitutional despite using “a definition of ‘probable cause’ that does not depend on

whether a domestic crime has been committed”); *United States v. Cavanagh*, 807 F.2d 787, 790–91 (9th Cir. 1987) (ruling that Fourth Amendment’s probable cause and particularity requirements are satisfied for an order targeting a facility used by a foreign power); *El-Mezain*, 664 F.3d at 568–70; *Abu-Jihaad*, 630 F.3d at 117–19; *United States v. Isa*, 923 F.2d 1300, 1304 (8th Cir. 1991). FISA’s “significant purpose” standard is also constitutional under the Fourth Amendment. *See United States v. Duka*, 671 F.3d 329, 343–45 (3d Cir. 2011).

Furthermore, the certifications submitted in support of a FISA application should be “subjected only to minimal scrutiny by the courts,” *United States v. Badia*, 827 F.2d 1458, 1463 (11th Cir. 1987), and are to be “presumed valid.” *Duggan*, 743 F.2d at 77 & n.6 (citing *Franks*); *see also United States v. Turner*, 840 F.3d 336, 342 (7th Cir. 2016) (“In reviewing the adequacy of the FISA application, . . . our role ‘is not to second-guess the executive branch official’s certification’”) (quoting *In re Grand Jury Proceedings of the Special Apr. 2002 Grand Jury*, 347 F.3d 197, 204 (7th Cir. 2003)); *United States v. Campa*, 529 F.3d 980, 993 (11th Cir. 2008); *United States v. Kashmiri*, No. 09-CR-830-4, 2010 WL 4705159, at *1 (N.D. Ill. Nov. 10, 2010); *United States v. Sherifi*, 793 F. Supp. 2d 751, 760 (E.D.N.C. 2011) (“a presumption of validity [is] accorded to the certifications”); *United States v. Nicholson*, No. 09-CR-40-BR, 2010 WL 1641167, at *5 (D. Or., Apr. 21, 2010) (quoting *United States v. Rosen*, 447 F. Supp. 2d 538, 545 (E.D. Va. 2006)); *Warsame*, 547 F. Supp. 2d at 990 (“a presumption of validity [is] accorded to the certifications”). If the target is a United States person, then the district court should also ensure that each certification is not “clearly erroneous.” *Campa*, 529 F.3d at 994; *Duggan*, 743 F.2d at 77; *Kashmiri*, No.

09 CR 830-4, 2010 WL 4705159 at *2. A certification is clearly erroneous only when “the reviewing court on the [basis of the] entire evidence is left with the definite and firm conviction that a mistake has been committed.” *United States v. U.S. Gypsum Co.*, 333 U.S. 364, 395 (1948); see *United States v. Garcia*, 413 F.3d 201, 222 (2d Cir. 2005); *United States v. Islamic American Relief Agency (“IARA”)*, No. 07-00087-CR-W-NKL, 2009 WL 5169536, at *4 (W.D. Mo. Dec. 21, 2009). Applying these standards, this Court finds that the certification(s) at issue here were made in accordance with FISA’s requirements.

Although Defendant has not moved for an adversarial hearing pursuant to *Franks*, he seeks disclosure of the FISA materials so that he may pursue a *Franks* hearing. A defendant is entitled to such a *Franks* hearing only where he has made “a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included” in the FISA materials and that the allegedly false statement was necessary to the FISC’s approval of the application(s). See *Franks*, 438 U.S. at 155–56. Defendant has made no such showing here; he has not shown that any statement was false and has not shown that any such false statements were material, and made knowingly, intentionally, or with reckless disregard for their truth. As a result, he is not entitled to a *Franks* hearing. Although Defendant has not reviewed the FISA materials, the Court has independently reviewed all such materials and finds no indication of any false statements having been included in the FISA materials.

III. Conclusion

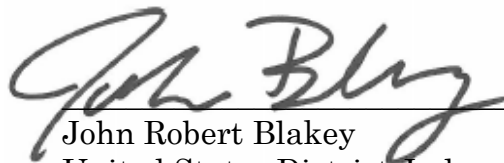
The Court finds that the government complied with its notice obligations under FISA when it notified Defendant and the Court on October 23, 2018 of its intent to “offer into evidence, or otherwise use or disclose in any proceeding in this matter, information obtained and derived from electronic surveillance and physical search” conducted pursuant to FISA. (50 U.S.C. §§ 1806(c) and 1825(d).) The Court further finds that Defendant is not entitled to additional notice or information regarding any surveillance techniques that may have been employed in this matter.

Accordingly, the Court denies Defendant’s Motions [222] and [223];

It is further ordered that the government’s FISA application(s), order(s), and other FISA-related materials (and its classified submissions for this matter) are SEALED and shall be retained in accordance with established security procedures by the Classified Information Security Officer or his/her designee.

Dated: May 4, 2021

ENTERED:

A handwritten signature in black ink, appearing to read "John Blakey", is written over a horizontal line.

John Robert Blakey
United States District Judge
Northern District of Illinois