IN THE UNITED STATES DISTRICT COURT WESTERN DISTRICT OF MISSOURI WESTERN DIVISION

UNITED STATES OF AMERICA)
Plaintiff,)
i iuiiviii,)
)
VS.) Case No. 07-00087-CR-W-NKL
)
ISLAMIC AMERICAN RELIEF)
AGENCY, et al.,	
)
Defendants.)

ORDER

Pending before the Court is a Motion to Obtain Disclosure of and Suppress Electronic Surveillance Evidence Obtained Pursuant to Foreign Intelligence Surveillance Act ("FISA") filed by Defendants Murabek Hamed, Ali Bagegni, and Ahmad Mustafa ("Defendants") [Doc. # 191]. In their Motion, Defendants seek disclosure of FISA applications, orders, and relevant related materials to determine whether Defendants' surveillance was lawfully authorized and conducted. Defendants further seek suppression of any such evidence obtained unlawfully. They also assert that the FISA collection violated their Fourth Amendment right because of a change made to the statute by the USA PATRIOT Act of 2001 ("Patriot Act"). For the reasons stated below, the Court denies Defendants' Motion.

I. Background

Defendants are charged with crimes related to 1) the illegal transfer and attempted transfer of funds to Iraq, 2) the transfer of funds to Pakistan for the benefit of a Specially

Designated Global Terrorist, 3) the misuse of funds received from the United States Agency for International Development, and 4) obstructing or impeding the administration of tax laws in various counts of a forty-two count Indictment. The Government previously notified Defendants that it intended to introduce evidence that was obtained or derived from searches authorized by the United States Foreign Intelligence Surveillance Court ("FISC"). Defendants now seek disclosure of FISA applications, orders, and other materials relied on by the FISC in authorizing the searches. They also seek suppression of any materials obtained unlawfully. In response to this motion, the Government submitted classified dockets of the materials underlying the FISA warrants at issue in this case for the Court's *in camera* review. The Government also publicly filed unclassified versions of its briefing. [Docs. ## 282, 326].

II. Discussion

A. Foreign Intelligence Surveillance Act Statutory Scheme

At issue in this case is whether FISA orders of surveillance in this case were properly authorized, and whether the FISA collection was lawfully conducted. FISA was enacted in 1978 and established procedures regarding the Executive Branch's collection of foreign intelligence information. Prior to the enactment of FISA, Presidents "had claimed inherent power to conduct warrantless electronic surveillance in order to gather foreign intelligence in the interests of national security." *ACLU Found. of S. Cal. v. Barr*, 952 F.2d 457, 461 (D.C. Cir. 1991). The enactment of FISA "sought to put to rest a troubling constitutional

electronic surveillance in the foreign intelligence context. *United States v. United States District Court (Keith)*, 407 U.S. 297, 321-22 (1972) (expressly declining to determine whether the Fourth Amendment limited the President's ability to obtain foreign intelligence through electronic surveillance). "By enacting FISA, Congress sought to resolve doubts about the constitutionality of warrantless, foreign security surveillance and yet protect the interests of the United States in obtaining vital intelligence about foreign powers." *Barr*, 952 F.2d at 461.

FISA created the United States Foreign Intelligence Surveillance Court, consisting of federal district court judges appointed by the Chief Justice of the Supreme Court. 50 U.S.C. § 1803(a). These judges review applications for authorization of electronic surveillance or physical searches sought for foreign intelligence purposes. 50 U.S.C. §§ 1803, 1822(c). Although there are several exceptions, "electronic surveillance of a foreign power or its agents may not be conducted unless the FISC authorizes it in advance." *Barr*, 952 F.2d at 461.

To obtain authorization to conduct surveillance or physical searches, FISA requires the Government to file an *ex parte* application, under seal, with the FISC. 50 U.S.C. §§ 1804, 1823. The application must be made by a federal officer in writing and under oath and must be approved by the Attorney General. Most important to the Defendants' motion in this case, the application must include certain certifications, a probable cause statement, and a

statement of proposed minimization procedures, which must be followed in the collection of FISA materials. *Id.* These requirements as applied in this case will be discussed in the Court's analysis regarding whether the FISA collection was properly authorized (certifications and probable cause analysis) and whether the FISA collection was properly conducted (minimization procedures analysis) in more detail below. *See infra* II.C.

The application is reviewed by a single judge in the FISC, and upon approval of the Government's application, the judge's order granting the application must reflect that the Government satisfied the FISA statute's requirements. The order must also describe, among other things, the target, information sought, and means of acquiring any such information. 50 U.S.C. §§ 1805(c)(1), 1824(c)(1). The order also sets forth the period of time during which the surveillance is approved, usually ninety days, and can be extended upon an application. *Id.* § 1805(e)(1). When obtaining foreign intelligence information, FISA also "specifically contemplates cooperation between federal authorities conducting electronic surveillance and physical searches pursuant to FISA and federal law enforcement officers investigating clandestine intelligence activities" and "explicitly allows the use of evidence derived from FISA surveillance and searches in criminal prosecutions." *United States v. Rosen*, 447 F. Supp. 2d 538, 544 (E.D. Va. 2006) (citing 50 U.S.C. §§ 1806(k), 1825(k)).

If the Attorney General approves use of evidence collected under FISA in a criminal prosecution, and the Government intends to use such evidence at the trial of an "aggrieved

person,"¹ then the Government must notify the aggrieved person and the district court of this intention. 50 U.S.C. § 1806(c). In this case, the Government has provided such notice and the parties agree that Defendants are "aggrieved persons." As a result of this notice, Defendants may move to suppress the use of FISA materials on two grounds: (1) the information was unlawfully acquired; or (2) the electronic surveillance or physical searches were not conducted in conformity with an order of authorization or approval by the FISC. 50 U.S.C. §§ 1806(e), 1825(f); see also United States v. Isa, 923 F.2d 1300, 1303 (8th Cir. 1991). Defendants also argue that the FISA surveillance in this case violated their Fourth Amendment Rights because foreign intelligence must be the "primary purpose" of the surveillance rather than a "significant purpose" as redefined by the Patriot Act.²

B. Motion for Disclosure of FISA Materials

Defendants seek disclosure of FISA materials so that they can review them and to develop their arguments for their motion to suppress. Defendants correctly explain that an *ex parte* review of FISA materials is not necessary unless the Attorney General files an affidavit stating that "disclosure or an adversary hearing would harm the national security of

¹An "aggrieved person" with regard to electronic surveillance is defined as "a person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance." 50 U.S.C. § 1801(k). With regard to physical searches, an "aggrieved person" is "a person whose premises, property, information, or material is the target of physical search or any other person whose premises, property, information, or material was subjected to physical search." *Id.* § 1821(2).

²This argument was not presented by Defendants until their reply brief. [Doc. # 299]. However, the Court will address the issue because it has been fully briefed after the Government's surreply.

the United States." [Doc. # 260, p. 1]. In response to the motion, the Government filed such an affidavit in which the Attorney General explains that disclosure of the FISA dockets in this case "reasonably could be expected to cause serious damage to national security of the United States." [Doc. # 282-1, p. 3].

Once this affidavit is filed, FISA provides that Courts must first review the challenged dockets ex parte and in camera and may review and disclose FISA applications and related materials "only where such disclosure is necessary to make an accurate determination of the legality of the surveillance." 50 U.S.C. § 1806(f). Both parties agree that no court has ever ordered such disclosures. United States v. Warsame, 547 F. Supp. 2d 982, 987 (D. Minn. 2008) ("No United States District Court or Court of Appeals has ever determined that disclosure to the defense of such materials was necessary to determine the lawfulness of surveillance or searches under FISA."); see also Rosen, 447 F. Supp. 2d at 546 (collecting cases). Moreover, the constitutionality of FISA's provisions regarding the Court's ex parte, in camera review has been affirmed by federal courts, including the Eighth Circuit, to consider the issue. See, e.g., Isa, 923 F.2d at 1307 (holding that FISA's review procedures do not violate a defendant's Sixth Amendment right to confrontation); United States v. Damrah, 412 F.3d 618, 624 (6th Cir. 2005) ("FISA's requirements that the district court conduct an ex parte, in camera review of FISA materials does not deprive a defendant of due process.").

Defendants argue that FISA expressly grants courts discretion to review materials and

disclose such documents to the defense as appropriate. The Government responds that the rationale for non-disclosure is clear: "In the sensitive area of foreign intelligence gathering, the need for extreme caution and sometimes even secrecy may not be overemphasized." *United States v. Ott*, 637 F. Supp. 62, 65 (E.D. Cal. 1986).

The Court concludes that its careful review of the FISA materials is sufficient to determine whether the FISA warrants were lawfully authorized and conducted. FISA's legislative history also supports this conclusion. Referencing FISA's legislative history, one court has concluded that disclosure would be "necessary" only

where the court's initial review of the application, order, and fruits of the surveillance indicates that the question of legality may be complicated by factors such as "indications of possible misrepresentation of fact, vague identification of the persons to be surveilled, or surveillance records which include a significant amount of nonforeign intelligence information, calling into question compliance with the minimization standards contained in the order."

United States v. Belfield, 692 F.2d 141, 147 (D.C. Cir. 1982) (quoting S. Rep. No. 95-701, 95th Cong., 2d Sess. 64 (1978)). Defendants argue in favor of disclosure of the FISA materials claiming that the Government's disclosure to them of intercepted telephone calls and documents demonstrate that there is "a significant amount of non-foreign intelligence information [] included in the records." [Doc. # 260, p. 3]. Although Defendants have concerns regarding the amount of non-foreign intelligence included in the records, the Court, after conducting a searching, comprehensive, and careful review of all the FISA materials in this case, finds that disclosure is not

C. Motion to Suppress

In their motion to suppress, Defendants argue that the FISA surveillance in this case was neither lawfully authorized nor conducted properly. With regard to whether the FISA surveillance was properly authorized, the Court reviewed the contents of the certifications in the FISA applications and the probable cause determinations of the FISC. It made a *de novo* review because the original review was "ex parte and thus unaided by the adversarial process." See, e.g., Rosen, 447 F. Supp. 2d at 545 (citing United States v. Hammoud, 381 F.3d 316, 332 (4th Cir. 2004); United States v. Squillacote, 221 F.3d 542, 554 (4th Cir. 2000)). No deference was accorded to the FISC's probable cause determination but, there is a presumption of validity accorded to the certifications. See 50 U.S.C. § 1805(a)(5). The Court also conducted a review of the minimization procedures applied in this case.

1. Lawfully Authorized

a. Certifications

Defendants argue that the certifications should be reviewed to determine whether they satisfy the statutory requirements of 50 U.S.C. § 1805(a). Because Defendants are United States persons,³ the Court must determine whether the certifications in the FISA applications are clearly erroneous. *See* 50 U.S.C. 1805(a)(5). A "clearly erroneous" finding is established

³ Under FISA, a "United States person" means, among other things, a "citizen of the United States, an alien lawfully admitted for permanent residence" 50 U.S.C. § 1801(i). Defendants assert that each are United States citizens, except Mustafa. However, they do not argue that Mustafa is not a "United States person" as defined by FISA. Thus, the Court assumes all Defendants are United States persons as defined by FISA.

when "although there is evidence to support it, the reviewing court on the entire evidence is left with the definite and firm conviction that a mistake has been committed." *United States* v. *United States Gypsum Co.*, 333 U.S. 364, 395 (1948).

After a careful review of the FISA materials in this case, the Court concludes that the applications and the FISC orders that resulted satisfy the requirements of 50 U.S.C. § 1805(a). The Attorney General was authorized by the President to approve applications to the FISC. Further, the Court's independent review of all the applications submitted to it reveals that the certifications were not clearly erroneous. *See United States v. Duggan*, 743 F.2d 59, 77 (2d Cir. 1984) ("The 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."); *United States v. Campa*, 539 F.3d 980, 993 (11th Cir. 2008) ("The reviewing court has no greater authority to review the certifications of the executive branch than the FISA court has."). As a result, Defendants' motion to suppress based on the FISA certifications is denied.

b. Probable Cause

The Court must next determine whether the FISC orders were supported by probable cause. "The showing of probable cause necessary to justify a FISA surveillance or search is not necessarily analogous to the probable cause standard applicable to the general criminal context." *United States v. Ahmed*, No. 06-147, slip op. at 18 (N.D. Ga. Mar. 19, 2009) (citing *United States v. Cavanagh*, 807 F.2d 787, 790 (9th Cir. 1987)). In a criminal case, the judge

makes a "practical, common-sense decision whether, given all the circumstances set forth in the affidavit . . . there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Illinois v. Gates*, 462 U.S. 213, 238 (1983). However, under Congress' statutory scheme, a FISA judge must determine that there is probable cause to believe that "the target of the electronic surveillance is a foreign power or an agent of a foreign power" and that "each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power." 50 U.S.C. § 1804(a)(3).

After a searching, comprehensive, and careful review, the Court finds that the warrants issued by the FISC were supported by probable cause. The supporting applications showed probable cause that Defendants IARA and Hamed were agents of a foreign power and that the facilities at which the surveillance would be directed were being used or about to be used by Defendants IARA and/or Hamed. Accordingly, the Court declines to grant Defendants' motion to suppress based on insufficient probable cause for the issuance of the FISA warrants.

2. Lawfully Conducted-Minimization Procedures

Defendants also challenge the FISA evidence, arguing that the Government failed to follow proper minimization procedures because the documents produced to them by the Government contain a "significant amount of non-foreign intelligence information." [Doc. # 260, p. 3.] In accordance with FISA's requirements, the Attorney General has adopted

standard minimization procedures. Although the specific procedures for each application are classified, the minimization procedures adopted by the Attorney General must meet the definition of minimization procedures under FISA. *See* 50 U.S.C. §§ 1801(h), 1821. FISA provides the following guidance with regard to the procedures that must be adopted:

- (1) specific procedures, which shall be adopted by the Attorney General, that are 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;
- (2) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in subsection (e)(1) of this section, shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance;
- (3) notwithstanding paragraphs (1) and (2), 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; and
- (4) notwithstanding paragraphs (1), (2), and (3), with respect to any electronic surveillance approved pursuant to section 1802(a) of this title, procedures that require that no contents of any communication to which a United States person is a party shall be disclosed, disseminated, or used for any purpose or retained for longer than 72 hours unless a court order under section 1805 of this title is obtained or unless the Attorney General determines that the information indicates a threat of death or serious bodily harm to any person.
- Id. § 1801(h); see also § 1821(4). Such procedures "are designed to protect, as far as reasonable, against the acquisition, retention and dissemination of nonpublic information which is not foreign intelligence information." In re Sealed Case, 310 F.3d 717, 731

(Foreign Int. Surv. Ct. Rev. 2002). Moreover, in reviewing the legislative history of FISA, one court has explained that "minimization may occur at any of several stages, including recording, logging, indexing, or dissemination." *In re Kevork*, 634 F. Supp. 1002, 1017 (C.D. Cal. 1985).

Under FISA, the extent of the minimization depends on the construction of "foreign intelligence information," which is defined as:

- (1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against--(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; (B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or
- (2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to--(A) the national defense or the security of the United States; or (B) the conduct of the foreign affairs of the United States.

50 U.S.C. § 1801(e). Courts have construed this definition broadly. *See, e.g., Rosen*, 447 F. Supp. 2d at 551 ("Acknowledging the inherent difficulty in determining whether something is related to clandestine activity, courts have construed 'foreign intelligence information' broadly and sensibly [and] allowed the government some latitude in its determination of what is foreign intelligence information.").

In assessing the Government's minimization efforts in this case, "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." See S.

Rep. No. 95-701, at 39-40 (1978), 1978 U.S.C.C.A.N. 3973, 3990-91 (quoting *United States v. Tortorello*, 480 F.2d 764 (2d Cir. 1973)). "Absent a charge that the minimization procedures have been disregarded completely, the test of compliance is 'whether a good faith effort to minimize was attempted." *Id.* (quoting *United States v. Armocida*, 515 F.2d 29, 44 (3d Cir. 1975)). Moreover, one court, in reviewing FISA dockets and concluding that there was proper minimization explained, "[t]he *ex parte, in camera* review of the FISA dockets discloses that any failures to minimize properly the electronic surveillance of the defendants were (i) inadvertent, (ii) disclosed to the FISC on discovery, and (iii) promptly rectified." *Rosen*, 447 F. Supp. 2d at 552.

Defendants argue that certain documents produced to them in discovery, such as "faxes and e-mails include personal correspondence, matters related to management of the local Mosque, news releases and commercial advertisements" do not constitute foreign intelligence information. *See* Doc. # 299, at p. 3. Defendants submitted a sampling of such documents and assert that such documents come from more than 4,000 documents with Bates Number beginning "FFAX." *Id.* at p. 4; Doc. # 300, Ex. A. Many of these documents are clearly not foreign intelligence information as they are, for example, generic advertisement for computers, vacations, etc.

This Court has conducted a searching, comprehensive, and thorough review of the FISA dockets in this case, and the documents that Defendants assert were not properly minimized. However, even if such documents were not properly minimized, Defendants fail to

demonstrate the remedy for such failure would be suppression of all documents obtained by the government pursuant to its FISA warrants. Rather, the legislative history for FISA explains

[a]s 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.

H.R. Rep. No. 95-1283, 95th Cong., 2d Sess., Pt. 1 at 95. Accordingly, this Court declines to suppress evidence obtained through FISA warrants properly issued and conducted.

D. Fourth Amendment and FISA's "Significant Purpose" Requirement

Defendants argue that the FISA surveillance in this case violated their Fourth Amendment rights because foreign intelligence must be the "primary purpose" of the surveillance rather than a "significant purpose" as redefined by the Patriot Act. If the primary purpose of the surveillance was not for foreign intelligence, then Defendants argue that the materials obtained pursuant to the FISA warrants issued in this case constituted an unreasonable search and seizure. This issue has not been addressed by the Eighth Circuit, and only one other district court in this circuit has addressed the issue.

See Warsame, 547 F. Supp. 2d at 994-97.

Prior to the enactment of the Patriot Act, one of the requirements of the application for a FISA warrant was a certification to the FISA judge "that the purpose of the surveillance is to obtain foreign intelligence information." 50 U.S.C. § 1804(a)(7)(B) (2000). Courts have interpreted "the purpose" language to require a showing that "the

primary purpose" of the surveillance was to obtain foreign intelligence. *Warsame*, 547 F. Supp. 2d at 995 (citing *Duggan*, 743 F.2d at 77; *United States v. Johnson*, 952 F.2d 565, 572 (1st Cir. 1991)). "The 'primary purpose' requirement ensured that law enforcement officials availed themselves of FISA's more flexible certification procedures only if the primary purpose sought to obtain foreign intelligence information." *Id.* The "primary purpose" requirement was to prevent an end-run around the more stringent requirements of a Title III warrant and the Fourth Amendment in the context of an ordinary criminal investigation. *Id.* (citing *Johnson*, 952 F.2d at 572).

The Patriot Act amended this language by requiring that "a significant purpose" for the surveillance be foreign intelligence information gathering. As a result of this change, "FISA now allows surveillance and searches even where the primary purpose of the surveillance is criminal prosecution, so long as 'a significant purpose' of the surveillance is to obtain foreign intelligence." *Id.* at 995 (citing *In re Sealed Case*, 310 F.3d at 732-33). All except one court to interpret this amendment have held that it complies with requirements of the Fourth Amendment. *See, e.g., In re Sealed Case*, 310 F.3d at 736-46; *United States v. Damrah*, 412 F.3d at 625; *United States v. Benkahla*, 437 F. Supp. 2d 541 (E.D. Va. 2006); *United States v. Abu-Jihaad*, 531 F. Supp. 2d 299, 304 (D. Conn. 2008). Only one district court has concluded that it does not. *Mayfield v. United States*, 504 F. Supp. 2d 1023, 1042-43 (D. Or. 2007) (concluding that the "significant purpose" requirement in the Patriot Act is unconstitutional under the Fourth

Amendment).

Without deciding whether the "significant purpose" test violates the Defendants'

Fourth Amendment rights, the Court finds, even if the primary purpose test applies, it is

satisfied in this case. The information contained in the applications supports a conclusion

that investigators were primarily interested in obtaining foreign intelligence information.

Accordingly, Defendants' motion to suppress the FISA materials in this case is denied.

III. Conclusion

Accordingly, it is hereby ORDERED that Defendants' Motion to Obtain

Disclosure of and Suppress Electronic Surveillance Evidence Obtained Pursuant to

Foreign Intelligence Surveillance Act [Doc. # 191] is DENIED.

s/ Nanette K. Laughrey

NANETTE K. LAUGHREY

United States District Judge

Dated: December 21, 2009

Jefferson City, Missouri

16