UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

United States of America,

Plaintiff,

v.

MEMORANDUM OPINION AND ORDER
Criminal No. 11-191

Ahmed Hussein Mahamud,

Defendant.

John Docherty and Charles Kovats, Assistant United States Attorneys and William M. Narus, U.S. Department of Justice, Counsel for Plaintiff.

Rick E. Mattox, Mattox Law Office, Counsel for Defendant.

Defendant has been charged by Indictment with conspiracy to provide, and providing, material support to terrorists and conspiracy to provide, and providing, material support to a Foreign Terrorist Organization ("FTO"). The government has provided notice to the Court and to the Defendant pursuant to 50 U.S.C § 1806(c) and 1825(d) that it intends to introduce at trial evidence obtained and derived from electronic surveillance, 50 U.S.C. § 1801-1812, and evidence obtained from physical searches. 50 U.S.C. § 1821-1829.

Defendant has filed a motion to suppress any evidence illegally obtained by wire surveillance, based on intercepted electronic communications obtained under the Foreign Intelligence Surveillance Act ("FISA"), 50 U.S.C. § 1801 et seq., and has moved for disclosure of all evidence related to the electronic surveillance. (Doc. Nos. 39 and 40.) In response, the government has filed a classified, as well as a redacted, unclassified memorandum opposing the motions. The Defendant's motions have triggered this Court's review of the FISA applications and orders pursuant to 50 U.S.C. § 1806(f) to determine whether the surveillance was lawfully authorized and conducted.

I. Foreign Intelligence Surveillance Act

FISA governs electronic surveillance and physical searches within the United States for foreign intelligence purposes. Each application for a warrant pursuant to FISA shall include the following:

> (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 relied upon by the applicant to justify his belief that--
>
> (A) the target of the electronic surveillance is a foreign power or an

> agent of a foreign power; and
>
> (B) 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;
>
> (4) a statement of the proposed minimization procedures;
>
> (5) a description of the nature of the information sought and the type of communications or activities to be subjected to the surveillance. . .

50 U.S.C. § 1804(a).

The application should also include a certification from the appropriate official

> (A) that the certifying official deems the information sought to be foreign intelligence information;
>
> (B) that a significant purpose of the surveillance is to obtain foreign intelligence information;
>
> (C) that such information cannot reasonably be obtained by normal investigative techniques;
>
> (D) that designates the type of foreign intelligence information being sought according to the categories described in section 1801(e) of this title; and
>
> (E) including 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 . . .

Id. § 1804 (6).

Finally, the application should include a summary of the surveillance to be conducted and whether a physical entry is required, whether "previous applications that have been made to any judge under this subchapter involving any of the persons, facilities, or places specified in the application, and the action taken on each previous application" and the time period for which surveillance is needed. Id. § 1804 (a)(7)-(9).

When reviewing a request for a warrant, the FISA Court must find probable cause to believe that the target of the surveillance is a 'foreign power or an agent of a foreign power' and that the place or facilities to be surveilled are 'being used, or ... about to be used, by a foreign power or an agent of a foreign power.'" United States v. Abu-Jihaad, 630 F.3d 102, 117-18 (2d Cir. 2010) (quoting 50 U.S.C. § 1805(a)(2)).

FISA further provides that the target of surveillance "may move to suppress the evidence on the grounds that [it] was unlawfully acquired or the surveillance was not made in conformity with [a FISA] order . . ." 50 U.S.C. §

1806(e). Where such a motion is filed, or a motion to discover or obtain FISA applications or orders is made, the court must, upon the filing of an affidavit from the Attorney General that disclosure of such material or an adversary hearing would harm national security,

> 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.

Section 1806(f).

II. Motion to Disclose

Defendant moves for an Order directing the government to disclose and to certify the extent of electronic surveillance used by the government in any phase of its investigation of him. Disclosure of such materials is warranted "only where such disclosure is necessary to make an accurate determination of the legality of the surveillance." 50 U.S.C. § 1806(f). Where 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." Id. (citing 50 U.S.C. § 1806(g)). Disclosure is thus "the exception and *ex parte*, *in camera* determination is the rule. Abu-Jihaad, 630 F.3d at 129 (internal

citations omitted).

In this case, Attorney General Eric Holder has filed an affidavit dated January 5 2012, declaring that disclosure of classified material or an adversary proceeding concerning such material would harm national security. (Government's Memorandum in Opposition, Exhibit 1) The Court has thus conducted an *ex parte, in camera* review of the applicable FISA applications, orders and related materials as provided in § 1806(f).

In determining whether disclosure is necessary, the Court should consider whether, after its initial review, any irregularities are revealed, such as whether: the materials evidence a possible misrepresentation of fact; the persons to be surveilled are not clearly identified; or the surveillance records include a significant amount of nonforeign intelligence information, indicating a possible issue with the minimization standards utilized. United States v. Warsame, 547 F. Supp.2d 982, 987 (D. Minn. 2008) (quoting United States v. Belfield, 692 F.2d 141, 147 (D.C. Cir. 1982)). Based on its *ex parte, in camera* review, no such irregularities were revealed. The Court thus finds that disclosure of the materials is not necessary to make an accurate determination of the legality of the surveillance.

III. Motion to Suppress

Defendant has moved to suppress any evidence obtained directly or indirectly from the interception of electronic communications on the grounds that such interceptions were obtained in violation of his rights under the Fourth Amendment and his legal rights under 18 U.S.C. § 2510 and 50 U.S.C. § 1806(e). Defendant furthers argue that to the extent the government offers information to the Court *in camera* on the legal authority to intercept communications in this case, the Defendant objects that such proceedings deprive him of his rights to due process under the Fifth Amendment.

A. Statutory Requirements

When reviewing FISA applications and orders to determine compliance with FISA procedures, the Court must keep in mind that "FISA warrants are subject to 'minimal scrutiny by the courts,' both upon initial presentation and subsequent challenge." Abu-Jihaad, 630 F.3d at 130 (quoting United States v. Duggan, 743 F.2d 59, 77 (2d Cir. 1984)). When reviewing a FISA warrant, the FISA Court considers whether the application makes the proper probable cause showing that the target of the warrant is a foreign power or an agent of a foreign power and that the facilities or places to be searched or surveilled are being used

by the foreign power/agent, whether the application is otherwise proper, and when the target is a United States citizen, whether the application's certifications are not clearly erroneous. Id. When reviewing a FISA Court Order, the reviewing court must presume as valid "'the representations and certifications submitted in support of an application for FISA surveillance . . . '" absent a showing sufficient to trigger a Franks hearing[1]." Id.

With this standard in mind, the Court has thoroughly reviewed the FISA applications, orders and related materials, as well as the government's classified memorandum in opposition to the motions to suppress and for disclosure. As discussed below, the Court finds that both the applications and orders complied with all requirements set forth in 50 U.S.C. § 1805(a) and there has been no showing to trigger a Franks hearing.

1. Certification

The FISA applications and orders in this case satisfy the statutory requirements set forth in 50 U.S.C. §§ 1804(a) and 1805(a). The applications were

[1]In Franks v. Delaware, the United States Supreme Court held that to be entitled to a hearing to challenge the veracity of a warrant affidavit, a defendant must first make a showing that the affidavit contains deliberate falsehoods or statements made with a reckless disregard of the truth, and an accompanying offer of proof. 438 U.S. 154, 171 (1978).

made by a federal officer and were approved by the Attorney General or his authorized designate. Further, the applications contain the required statements and certifications. Also, no showing has been made which provides a basis to find that any of the facts contained in the FISA application are false or were made with reckless disregard for the truth.

2. Minimization Procedures

The minimization procedures contained in the FISA applications must comply with Section 1801(h), which provides:

> "Minimization procedures", with respect to electronic surveillance, means--
>
> (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.

After carefully reviewing the minimization procedures described in the FISA applications, the Court finds that such procedures comply with the statutory requirements set forth in Section 1801(h). The Court further finds that the government followed these procedures to appropriately minimize the information it obtained.

3. Probable Cause

In reviewing a FISA application, the FISA Court is to determine whether the application establishes probable cause that "A) the target of the electronic surveillance is a foreign power or an agent of a foreign power: Provided, That no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment to the

Constitution of the United States; and (B) 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. § 1805(a)(2).

In making the probable cause determination, the FISA Court may also "consider past activities of the target, as well as facts and circumstances relating to current or future activities of the target." Id. § 1805(b). "Foreign power" is not limited to a foreign government, it also includes a "group engaged in international terrorism or activities in preparation therefor." §§ 1801 (a) and 1821(1). Further, an "agent of a foreign power" is one who "knowingly engages in sabotage or international terrorism, or activities in preparation therefor, for or on behalf of a foreign power" and "anyone who knowingly aids, abets, or conspires with any person to engage in the activities described in the Act." Id. §§ 1801(b)(2) and 1821(1). Finally, "international terrorism" is defined as including conduct that "involve[s] a violent act[] or act[] dangerous to human life that are a violation of the criminal laws of the United States" that appears intended to "intimidate or coerce a civilian population; to influence the policy of a government by intimidation or coercion; or to affect the conduct of a government by assassination or kidnaping; and occurs totally outside the United States or

transcend national boundaries." Id. §§ 1801(c) and 1821(1).

There is no agreement among the federal courts as to whether the probable cause determination is made *de novo* or if a deferential standard is applied. See Abu-Jihaad, 630 F.3d at 130; Warsame, 547 F. Supp.2d at 990 (court reviewed probable cause determination *de novo*, given that the Court's review is *ex parte*). Even applying a *de novo* review, however, the Court finds that there was sufficient probable cause set forth in the applications and related materials that Defendant was an agent of a foreign power, al-Shabaab, and that the places to be searched or to be surveilled were being used by Defendant.

D. Timing

Finally, Defendant raises concern that the government did not follow the time limits of surveillance. Based on its *ex parte, in camera* review, the Court finds that the government complied with the time limits of surveillance set forth in the applicable orders.

Based on the above, the Court finds that Defendant's motion to suppress any evidence obtained directly or indirectly from the interception of electronic communications on the grounds that the FISA applications and orders did not meet the statutory requirements of FISA must be denied.

B. Fourth Amendment

Defendant argues that any evidence obtained directly or indirectly from the interception of electronic communications should be suppressed as such evidence was obtained in violation of his Fourth Amendment rights. To the extent that Defendant's motion is based on the arguably lower probable cause standard applied to FISA applications, many courts, including the Eighth Circuit, have found that the probable cause standard set forth in FISA does not violate the Fourth Amendment. See United States v. Duka, __ F.3d __, 2011 WL 6794022, at *4 (3d Cir. Dec. 28, 2011) (rejecting defendant's constitutional challenges to FISA under the Fourth Amendment); Abu-Jihaad, 630 F.3d at 120; United States v. Isa, 923 F.2d 1300, 1304 (8th Cir. 1991); Warsame, 547 F. Supp.2d at 993-94. Accordingly, to the extent the Defendant's constitutional challenge is based on the probable cause standard set forth in FISA, the motion must be denied.

To the extent that Defendant's motion is based on the argument that the "significant purpose" test violates the Fourth Amendment because there is no requirement of a probable cause showing that a crime is being committed, this argument has also been rejected by a number of courts. See, e.g., Dukas, 2011 WL 6794022, at *10; Abu-Jihaad, 630 F.3d at 127; Warsame, 547 F. Supp.2d at 995

(noting that courts addressing this issue, save one, have upheld FISA as consistent with the requirements of the Fourth Amendment). Based on the applicable law, the Court is satisfied that FISA's significant purpose requirement is consistent with the Fourth Amendment's protections against unreasonable searches and seizures.

C. Fifth Amendment

Defendant argues that to the extent the government intends to offer information to the Court *in camera* on their legal authority to intercept his communications, such procedure deprives him of his right to due process in violation of the Fifth Amendment. This argument has also been rejected on many occasions, on the basis that the *ex parte, in camera* review satisfies due process. See, e.g., Abu-Jihaad, 630 F.3d 129 (finding that the court's *ex parte, in camera* review permitted it to assess the legality of the surveillance and the requirements of due process did not counsel otherwise); United States v. Damrah, 412 F.3d 618, 624; United States v. Ott, 827 F.2d 473, 476-77 (9th Cir. 1987); Warsame, 547 F. Supp.2d at 988-89. This Court is also satisfied that its review of the FISA materials permitted the Court to adequately assess the legality of the surveillance, and that due process did not counsel otherwise. Accordingly, the

motion to suppress based on a violation of the Fifth Amendment will be denied.

IV. Motion for Discovery

Finally, Defendant seeks to inspect the facility where the original tapes or data was stored, and to inspect the sealing orders and logs for such data. Defendant does not provide any authority to support these requests. As discussed previously in this Memorandum Opinion, FISA prohibits disclosure of material obtained or derived thereunder, unless constitutionally required by due process or Brady v. Maryland.

In Isa, the Eighth Circuit rejected the argument that evidence obtained through FISA warrants should have been suppressed because the government did not provide minimization logs of the entire surveillance. 923 F.2d at 1305-06. The court found that FISA did "not require that a target be provided the minimization logs of the entire surveillance. Indeed, specific provisions of the Act suggest the contrary." Id. at 1306. Accordingly, this motion will be denied.

IT IS HEREBY ORDERED:

1. Defendant's Motion for Discovery and Inspection of Products and Records of Electronic Surveillance [Doc. No. 39] is DENIED to the extent the motion seeks classified material;

2. Defendant's Motion to Suppress Evidence Obtained by Wire Surveillance [Doc. No. 40] is DENIED.

Date: January 18, 2012

s/ Michael J. Davis
Michael J. Davis
Chief Judge
United States District Court

Criminal No. 11-191 (MJD/FLN)