UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES of AMERICA	)	
v.	)	
MUHAMED MUBAYYID, EMADEDDIN Z. MUNTASSER, and SAMIR AL-MONLA a/k/a SAMIR ALMONLA,	)	**Criminal No. 05-40026-FDS**
Defendants.	)	

MEMORANDUM AND ORDER ON DEFENDANTS' MOTIONS TO SUPPRESS EVIDENCE OBTAINED FROM FISA SEARCHES AND SURVEILLANCE AND FOR DISCLOSURE OR EX PARTE REVIEW OF MATERIALS RELATED TO FISA SEARCHES AND SURVEILLANCE

SAYLOR, J.

I. Background

This is a criminal prosecution under 18 U.S.C. § 371 (conspiracy to defraud the United States), 18 U.S.C. § 1001 (false statements), 26 U.S.C. § 7206(1) (false statements on tax returns), and 26 U.S.C. § 7212(a) (obstructing and impeding the Internal Revenue Service). In essence, the indictments charge that defendants Muhamed Mubayyid, Emadeddin Z. Muntasser, and Samir Al-Monla fraudulently obtained a charitable exemption under § 501(c)(3) of the Internal Revenue Code for an entity known as Care International, Inc. According to the indictments, defendants concealed that Care International was an outgrowth of and successor to the Al-Kifah Refugee Center, and that Care International solicited and distributed funds for, and issued publications supporting and promoting, Islamic holy war ("jihad") and holy warriors

("mujahideen").

During its investigation, the government obtained orders from the Foreign Intelligence Surveillance Court ("FISC") pursuant to the Foreign Intelligence Surveillance Act, as amended, 50 U.S.C. §§ 1801-1862 ("FISA").[1] The government's FISA applications, the affidavits related to those applications, the FISC orders, and the information obtained from surveillance and searches that were conducted in accordance with those orders are all classified as secret or top secret.

Defendants and their counsel have not been provided access to those FISA-related documents. The government has, however, provided defendants with a summary of materials derived from the electronic surveillance conducted pursuant to FISA. According to the government's representations, the FISA-based electronic surveillance of telephone calls and e-mails began on or before August 1994 and continued until at least April 2003. In addition, the government conducted one FISA-based physical search of a storage locker in October 2001.

Pending before the Court are three motions filed by defendants: a motion for disclosure or *ex parte* review of materials related to FISA surveillance and searches ("Mot. for Disclosure"), and two motions to suppress evidence obtained from FISA surveillance and searches and all fruits thereof ("Mot. to Supp." and "Al-Monla Mot. to Suppress"). In response, the government has filed (1) a classified *ex parte* brief in opposition to defendants' motions; (2) two unclassified briefs in opposition to defendants' motions; (3) a declaration and claim of privilege by the Attorney General of the United States; (4) three classified declarations by a high-ranking official of the FBI

[1] For a detailed summary of the procedures for obtaining FISA orders authorizing electronic surveillance or physical searches, *see generally United States v. Sattar*, No. 02 CR 395 JGK, 2003 WL 22137012, at *3-5 (S.D.N.Y. Sept. 15, 2003).

in support of the Attorney General's declaration and claim of privilege; (5) eight classified declarations by the FBI regarding the applicable minimization procedures; and (6) certified copies of the FISA materials. For the reasons set forth below, the motion to compel disclosure and the motions to suppress will be denied.

II. Motion to Compel Disclosure

Pursuant to 50 U.S.C. §§ 1806(f) and 1825(g), defendants have moved to compel the disclosure of classified materials related to the surveillance of defendants' communications and the search conducted pursuant to FISA, or, in the alternative, for an *ex parte* review of those materials. Defendants specifically request the disclosure of "any and all FISA applications, affidavits, court orders, and extensions, as well as any other documents related to the FISA searches and surveillance." (Mot. for Disclosure at 1). Defendants generally contend that they must have an opportunity to examine the FISA materials in order to file a factually specific motion to suppress and that disclosure is necessary to protect their rights to due process and effective assistance of counsel.

Under the statute, the Attorney General may oppose a request for disclosure by filing an affidavit stating that the disclosure "would harm the national security of the United States." 50 U.S.C. §§ 1806(f), 1825(g). The Attorney General has done so in this case. Upon the filing of such an affidavit, the Court must "review *in camera* and *ex parte* the application, order, and such other materials relating to the surveillance [or physical search] as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted," unless "disclosure is necessary to make an accurate determination of the legality of the surveillance." *Id.* §§ 1806(f), 1825(g); *see also United States v. Belfield*, 692 F.2d 141, 147 (D.C. Cir. 1982);

United States v. Johnson, No. 89-221-MA, 1990 WL 78522, at *2 (D. Mass. April 13, 1990), *aff'd*, 952 F.2d 565 (1st Cir. 1991).

The Court has reviewed the applications, orders, and other materials at issue *in camera* and *ex parte* to ensure that the surveillance was lawfully authorized and conducted. After reviewing these materials, the Court concludes that disclosure to defense counsel is not necessary in order to make an accurate determination of the legality of the government's surveillance and search.

It is of course true that the legality of the surveillance and search would be better tested through the adversarial process; an *ex parte* review is not a perfect substitute for that process. The question under the statute, however, is not how to optimize the legal review of the surveillance and search, but whether disclosure is "necessary" in order to make that determination. After careful review, the Court has concluded that such disclosure is not necessary, either in whole or in part. It is worth noting that, to date, every federal court that has considered a motion to disclose FISA applications or suppress FISA-based evidence appears to have reached a decision concerning the legality of the surveillance or search based on an *in camera* and *ex parte* review. *See, e.g., United States v. Damrah*, 412 F.3d 618, 624 (6th Cir. 2005); *United States v. Squillacote*, 221 F.3d 542, 553-54 (4th Cir. 2000); *United States v. Johnson*, 952 F.2d 565, 571-72 (1st Cir. 1991); *United States v. Isa*, 923 F.2d 1300, 1306 (8th Cir. 1991); *United States v. Sarkissian*, 841 F.2d 959, 964 (9th Cir. 1988); *United States v. Hawamda*, No. 89-56-A, 1989 WL 235836, at *1 (E.D. Va. April 17, 1989).

Defendants further request that the Court conduct an evidentiary hearing pursuant to *Franks v. Delaware*, 438 U.S. 154 (1978), in order to provide them with the opportunity to

"prove the affiants before the FISC intentionally or recklessly made materially false statements and omitted material information from the FISA applications." (Mot. to Suppress at 9-10). The Court assumes that *Franks*, or at least its underlying principle, applies in this context. *See United States v. Duggan*, 743 F.2d 59, 77 n.6 (2d Cir. 1984) (concluding that "the principles set forth in [*Franks*]" govern in FISA proceedings). Under *Franks*, however, in order to be entitled to a hearing, defendants must make "a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included" in the FISA application and that the allegedly false statement was "necessary" to the FISC's approval of the application. *Franks*, 438 U.S. at 155-56. Defendants have made no such showing here. *See Damrah*, 412 F.3d at 624-25 ("Even assuming that *Franks* applies to FISA applications and orders, Damrah's *Franks* attack was non-specific and unsupported."); *Duggan*, 743 F.2d at 77 n.6.

The Court obviously recognizes the difficulty of defendants' position: because they do not know what statements were made by the affidavit in the FISA applications, they cannot make any kind of a showing that those statements were false. *See Belfield*, 692 F.2d at 148. Nonetheless, it does not follow that defendants are entitled automatically to disclosure of the statements. The balance struck under FISA—which is intended to permit the gathering of foreign intelligence under conditions of strict secrecy, while providing for judicial review and other appropriate safeguards—would be substantially undermined if criminal defendants were granted a right of disclosure simply to ensure against the possibility of a *Franks* violation. As the court observed in *Belfield*:

We appreciate the difficulties of appellants' counsel in this case. They must argue

> that the determination of legality is so complex that an adversary hearing with full access to relevant materials is necessary. But without access to the relevant materials their claim of complexity can be given no concreteness. It is pure assertion.
>
> Congress was also aware of these difficulties. But it chose to resolve them through means other than mandatory disclosure. . . . [I]t cannot be said that this exclusion [of defendants from the process] rises to the level of a constitutional violation.

Id.; *see also United States v. Ott*, 827 F.2d 473, 476-77 (9th Cir. 1987) (no due process right to disclosure of FISA materials).

Accordingly, defendants' motion for disclosure of FISA-related materials will be denied, and their alternative motion for *ex parte* review by the Court will be granted.

III. Motion to Suppress

Defendants have further moved to suppress all fruits of the government's FISA-based surveillance and search. In substance, defendants make two arguments: first, that the government did not satisfy the statutory requirements when conducting its FISA-based surveillance and search, and second, that FISA is unconstitutional.

A. The FISA Statutory Requirements

1. Generally

In examining the adequacy of the FISA applications, certifications, and orders at issue, the Court reviewed the materials "*de novo* with no deference accorded to the FISC's probable cause determinations, but with a presumption of validity accorded to the certifications." *United States v. Rosen*, 447 F. Supp. 2d 538, 545 (E.D. Va. 2006); *see also United States v. Hammoud*, 381 F.3d 316, 332 (4th Cir. 2004) (conducting *de novo* review of FISA materials), *vacated on other grounds*, 543 U.S. 1097 (2005). In essence, this Court is required to conduct the same review of

the FISA materials that the FISC itself conducted. *See In re Grand Jury Proceedings of Special April 2002 Grand Jury*, 347 F.3d 197, 204-05 (7th Cir. 2003). In conducting that review, the Court may not simply second-guess the executive branch's certifications. *Duggan*, 743 F.2d at 77. As the *Duggan* court noted, "Congress intended that, when a person affected by a FISA surveillance challenges the FISA Court's order, a reviewing court is to have no greater authority to second-guess the executive branch's certifications than has the FISA Judge." *Id.* (*citing* H.R. Rep. No. 95-1283, pt. I, at 92-93 (1978)).

After reviewing the FISA materials at issue, and pursuant to the foregoing standard, the Court finds the following:

(1) the President has authorized the Attorney General to approve applications for electronic surveillance to the FISC (50 U.S.C. §§ 1805(a)(1), 1824(a)(1));

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

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

(5) each of the applications contained facts establishing probable cause to believe that each of the facilities or places at which the electronic surveillance was used at the time, or was about to be used at the time, by an agent of a foreign power and

the premises searched was owned, used, or possessed by an agent of a foreign power (50 U.S.C. §§ 1805(a)(3)(B), 1824(a)(3)(B));

(6) the minimization procedures included with the applications and orders of the judge met the requirements of § 1801(h) or § 1821(4) (50 U.S.C. §§ 1805(a)(4), 1824(a)(4));

(7) each application contained all statements and certifications required by § 1804 or § 1823 (50 U.S.C. §§ 1805(a)(5), 1824(a)(5));

(8) 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 § 1804(a)(7)(E) or § 1823(a)(7)(E) or any other facts furnished in the applications pursuant to § 1804(d) or § 1823(c) (50 U.S.C. §§ 1805(a)(5), 1824(a)(5)); and

(9) each of the orders issued by the FISC satisfied the requirements of § 1805(c) or § 1824(c).

Accordingly, the Court concludes that the FISC properly granted the FISA applications and issued FISA search and surveillance orders.

2. Minimization

The "minimization" requirement of the statute warrants separate discussion. FISA requires that the government undertake certain "minimization procedures" in the course of conducting electronic surveillance or a physical search under the statute. *See* 50 U.S.C. §§ 1805(a)(4), 1824(a)(4). In the case of electronic surveillance, "minimization procedures" are defined under the statute to mean specific procedures 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." *Id.* § 1801(h)(1); *see id.* § 1821(4)(A) (defining "minimization procedures" similarly for physical searches). A "statement of the proposed minimization procedures" must be included with an application for an order of surveillance or search. *Id.* §§ 1804(a)(5), 1823(a)(5).

The provision concerning surveillance further requires that "nonpublicly available information, which is not foreign intelligence information . . . 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." *Id.* §§ 1801(h)(2), 1821(4)(B). Notwithstanding those requirements, minimization procedures may "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." *Id.* §§ 1801(h)(3), 1821(4)(C).

As noted above, the Court has found that the minimization procedures employed by the government here met the requirements imposed by the statute. Defendant Al-Monla contends, however, that the minimization was necessarily inadequate, based on two asserted grounds.[2] First, he contends that the government has maintained copies of certain electronic surveillance going back to 1995, and therefore it appears that "there are no procedures for discarding irrelevant information, time restrictions, [or] deletion requirements, in violation of statutory

[2] Al-Monla requests that the Court prohibit the government from introducing at trial any communication intercepts based on the government's alleged violation of the minimization requirements.

directive." (Al-Monla Mot. to Suppress. at 24). Second, he contends that the government intercepted (and produced transcripts of) at least two conversations between Mubayyid and his wife, and therefore it appears that privileged communications were not minimized in any respect. *Id.* at 14.[3]

At the outset, the Court notes that the required minimization procedures apply only to communications of "unconsenting United States persons." Under FISA, an individual is a "United States person" if he is a citizen of the United States or an alien lawfully admitted for permanent residence in the United States. 50 U.S.C. § 1801(i). If defendants are not "United States persons," then the minimization procedures required under FISA do not apply. *See id.* §§ 1801(h)(1), 1821(4)(A).

The citizenship and immigration status of the three defendants is not entirely clear. Mubayyid is apparently a naturalized Australian citizen, of Lebanese origin, who was living in the United States pursuant to a work permit. Muntasser is apparently a citizen of Libya who is a permanent resident of the United States. Al-Monla is apparently a naturalized citizen of the United States, of Kuwaiti origin, who may also be a citizen of Lebanon.[4] Muntasser and Al-Monla appear to be "United States persons" for FISA purposes. Mubayyid, apparently, is not.[5]

---

[3] Al-Monla also states that "[d]uring one monitored call, on April 10, 2003, agents overheard conversations where the parties discussed the need for counsel in view of the government's actions and defendants told Suheil Laher that 'both lawyers actually suggested that you should also have a lawyer, Suheil.'" (Al-Monla Mot. to Suppress at 13-14). Those communications are not privileged, but may constitute "nonpublicly available information" that is not "foreign intelligence information."

[4] The Order Setting Conditions of Release for Al-Monla, issued on March 3, 2007, required him to surrender both his U.S. and Lebanese passports.

[5] Defendants contend, however, that "[a]t all relevant times, both Mr. Muntasser and Mr. Mubayyid were permanent resident aliens [of the United States]." (Mot. to Suppress at 5 n.3).

Neither the defendants nor the government have submitted evidence concerning defendants' citizenship or immigration status in connection with defendants' motions for disclosure and suppression.

In any event, even assuming that all three defendants are "United States persons," the Court cannot conclude that the minimization procedures here were either inappropriate or were not followed with sufficient fidelity. It is not fatal that the government may have recorded and stored an overbroad selection of communications; as the Fourth Circuit observed in *Hammoud*, 381 F.3d at 334:

> In enacting FISA, Congress recognized that "no electronic surveillance can be so conducted that innocent conversations can be totally eliminated." S.Rep. No. 95-701, at 39 (1978) (internal quotation marks omitted), *reprinted in* 1978 U.S.C.C.A.N. 3973, 4008. The minimization requirement obligates the Government to make a good faith effort to minimize the acquisition and retention of irrelevant information. *See id.* at 39-40. However, it is not always immediately clear into which category a particular conversation falls. A conversation that seems innocuous on one day may later turn out to be of great significance, particularly if the individuals involved are talking in code. In view of these considerations, the mere fact that innocent conversations were recorded, without more, does not establish that the government failed to appropriately minimize surveillance.

(citation omitted).

Nor is the fact that the information was stored for long periods necessarily problematic. The legislative history of FISA provides that

> in intelligence as in law enforcement, leads must be followed. Especially in counterintelligence cases where often trained professional foreign intelligence personnel are involved, a lead which initially ends in a "dry hole" can hardly be considered a dead issue, although it may be temporarily shelved to divert limited resources to other leads. Therefore, this committee intends that a significant degree of latitude be given in counterintelligence and counterterrorism cases with respect to the retention of information and the dissemination of information between and among counterintelligence components of the Government.

United States v. Thomson, 752 F. Supp. 75, 81-82 (W.D.N.Y. 1990) (*quoting* H.R. Rep. No. 95-1283, pt. I, at 59 (1978)); *see also In re Kevork*, 634 F. Supp. 1002, 1017 (C.D. Cal. 1985) (the government must be afforded flexibility "'with respect to the retention of information concerning U.S. persons [because] [i]nnocuous-sounding conversations may in fact be signals of important activity [and] information on its face innocent when analyzed or considered with other information may become critical.'" (*quoting* H.R. Rep. No. 95-1283, pt. I, at 55 (1978))), *aff'd on other grounds*, 788 F.2d 566 (9th Cir. 1986) .

In this case, the government apparently retained recordings of interceptions for more than ten years prior to indictment. It is important, however, to consider that fact in the proper context. The interceptions at issue were largely in a foreign language, and thus the information was not readily deciphered, analyzed, or catalogued. Furthermore, the Court must take into account the complex and time-intensive nature of piecing together, and making sense of, the myriad pieces of information gathered during a lengthy surveillance. In light of the "significant degree of latitude" given to the government in this respect, the Court concludes that the government's retention of the intercepts in this case does not violate FISA. *See* 50 U.S.C. §§ 1801(h), 1821(4).

As noted, Al-Monla also identifies two telephone calls between Mubayyid and his wife that the government monitored or recorded and transcribed. (Al-Monla Mot. to Suppress at 14).[6] In enacting FISA, Congress recognized that:

[6] Specifically, Al-Monla contends that during a monitored phone call, "Mubayyid told his wife, on February 3, 2003, that he was meeting with Care's accountant 'to go over the accounting papers for Care for last year.' His wife 'asked him why he is still working on things with Care and he told her that those are things from last year but should finish with them by the end of the month . . . and end it at the end of February.' On April 7, 2003, the day of the criminal searches, Mubayyid called his wife to say that agents were coming to search their home, and that he 'just want[ed] her to know so she does not get scared.'" (Al-Monla Mot. to Suppress at 14).

> As the courts have noted in construing [existing electronic surveillance law] "it is . . . obvious that no electronic surveillance can be so conducted that innocent conversations can be totally eliminated." *United States v. Bynum*, 485 F.2d 490, 500 (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." *United States v. Armocida*, 515 F.2d 29, 44 (3d Cir. 1975).

Thomson, 752 F. Supp. at 80 (*quoting* S. Rep. No. 95-701, at 39-40 (1978)).

Even assuming that the communications between Mubayyid and his wife are irrelevant and innocent—that is, they do not include foreign intelligence information or constitute communications in furtherance of a crime—the government's capture and transcription of the communications neither vitiates the government's FISA minimization procedures nor justifies suppressing the fruits of the government's surveillance. *See Sattar*, 2003 WL 22137012, at *10-11 (holding government's efforts at minimization reasonable and in good faith and in compliance with its reasonable procedures, despite intercepting allegedly non-pertinent calls between defendant and wife); *cf. United States v. Falcone*, 364 F. Supp. 877, 886 (D.N.J. 1973) (finding in analogous Title III context that "some non-pertinent, innocent, and unrelated calls may be received without causing suppression of the fruits of the electronic surveillance.") (citations omitted), *aff'd*, 500 F.2d 1401 (3d Cir. 1974).

Of course, the communications do not lose their privileged character (assuming they are privileged) simply by virtue of being intercepted. Thus, while the communications will not be excluded under FISA, the Court makes no ruling as to their admissibility at trial.[7]

[7] Al-Monla further contends that the renewed FISA orders were improper because the government utilized "normal investigative techniques" to investigate defendants during the same time period in which the government applied for, and was granted, the renewed orders. (Al-Monla Mot. to Suppress at 19-22). For an order to issue, FISA requires a high-ranking executive branch official to certify that the foreign intelligence information sought "cannot reasonably be obtained by normal investigative techniques." 50 U.S.C. §§ 1804(a)(7)(E)(ii),

B. Constitutionality of FISA

With one recent exception, every court to have considered the issue has ruled that FISA does not violate the Fourth Amendment. *See, e.g., United States v. Wen*, 477 F.3d 896, 898 (7th Cir. 2006); *Damrah*, 412 F.3d at 625; *American Civil Liberties Union v. United States Dep't of Justice*, 265 F. Supp. 2d 20, 32 & n.12 (D.D.C. 2003); *In re Sealed Case*, 310 F.3d at 742-46; *United States v. Pelton*, 835 F.2d 1067, 1075 (4th Cir. 1987); *United States v. Cavanagh*, 807 F.2d 787, 790-92 (9th Cir. 1987); *Duggan*, 743 F.2d at 77-78; *United States v. Holy Land Found. for Relief & Dev.*, No. 3:04-CR-240-G, 2007 WL 2011319, at *5-6 (N.D. Tex. July 11, 2007); *Sattar*, 2003 WL 22137012, at *12-13. *But see Mayfield v. United States*, 504 F. Supp. 2d 1023, 1036-43 (D. Or. 2007).

Defendants, however, contend that the FISA search and surveillance orders are not "warrants" within the meaning of the Fourth Amendment because they do not comply with the requirements of judicial review, probable cause, particularity, and notice. Defendants further contend that the "significant purpose" requirement set forth in the current version of FISA, as amended by the USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (Oct. 26, 2001) (the "Patriot Act"), violates the Fourth Amendment. The Court will address each argument in turn.

1. The Fourth Amendment's Judicial Review, Probable Cause, Particularity, and Notice Requirements

a. Judicial Review

1823(a)(7)(C). However, neither this certification requirement, nor any other FISA provision, precludes the government from using "normal investigative techniques" to seek evidence, while at the same time using FISA-based surveillance to seek foreign intelligence information that is otherwise unobtainable. *See In re Sealed Case*, 310 F.3d 717, 744 (F.I.S.C.R. 2002) (FISA-based surveillance and "the criminal process [are] often used as part of an integrated effort to counter the malign efforts of a foreign power."). Accordingly, the government's concurrent use of "normal investigative techniques" and FISA orders to seek different information does not violate the statute or otherwise render the FISA proceedings unlawful.

Defendants first contend that the governments' surveillance and search were conducted without meaningful prior judicial review, making them unreasonable under the Fourth Amendment. Defendants focus on the fact that the FISC must defer to the government's application certifications unless they are "clearly erroneous on the basis of the statement[s] made under § 1804(a)(7)(E) [or § 1823(a)(7)(E)]." 50 U.S.C. §§ 1805(a)(5), 1824(a)(5).[8]

Although judicial review of FISA applications is certainly more circumscribed than that of search warrant applications generally, it is far from a meaningless rubber-stamp. The requisite certifications must be made by high-ranking executive branch officials, providing an important check against reckless and arbitrary actions by law enforcement officers, particularly those in the field. Whatever the bounds of the "clearly erroneous" standard, a judicial officer plainly has the ability to deny a request intended solely for domestic law enforcement purposes, or where the foreign intelligence purpose is not significant. Furthermore, the statute provides the judicial officer the opportunity to require additional information. 50 U.S.C. §§ 1804(d), 1823(c). Under the circumstances, the Court agrees with the reasoning of the court in *In re Sealed Case*, 310 F.3d at 739, 746, that the judicial review required by the statute is reasonable within the meaning of the Fourth Amendment. *See also, e.g., Cavanagh*, 807 F.2d at 790 ("We conclude that appellant has failed to show that the FISA court provides anything other than neutral and responsible oversight of the government's activities in foreign intelligence surveillance."); *United States v. Spanjol*, 720 F. Supp. 55, 58 (E.D. Pa. 1989) ("FISA's procedure for obtaining judicial

[8] FISA presently requires that the certification be made by the Assistant to the President for National Security Affairs, or an executive branch official employed in the area of national security designated by the President, and that the Attorney General of the United States approve the certification. *See* 50 U.S.C. §§ 1804(a)(7), 1805(a)(2), 1824(a)(2).

authorization of the Government's electronic surveillance for foreign intelligence purposes interposes a neutral and detached judicial officer between the Government and the target of the surveillance. As such, it satisfies the warrant requirement of the Fourth Amendment."); *United States v. Megahey*, 553 F. Supp. 1180, 1190 (E.D.N.Y. 1982) ("[T]he FISA warrant is a warrant within the meaning of the fourth amendment, since it provides for the interposition of independent judicial magistrates between the executive and the subject of the surveillance which the warrant requirement was designed to assure."), *aff'd sub nom. United States v. Duggan*, 743 F.2d 59 (2d Cir. 1984).

b. Probable Cause

"'[P]robable cause is the standard by which a particular decision to search is tested against the constitutional mandate of reasonableness [and] [t]o apply this standard, it is obviously necessary . . . to focus upon the governmental interest which allegedly justifies official intrusion upon the constitutionally protected interests of the private citizen." *Camera v. Municipal Ct.*, 387 U.S. 523, 534-35 (1967). In FISA cases, the government interest is in protecting the United States and its citizens from "terrorists and espionage threats" by foreign powers or their agents. *In re Sealed Case*, 310 F.3d at 746.

FISA requires a showing of probable cause that the target of the surveillance or search 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 and that the premises to be searched is owned, used, or possessed by an

agent of a foreign power. 50 U.S.C. §§ 1805(a)(3), 1824(a)(3).[9] By contrast, for an electronic surveillance warrant to issue under Title III, there must be probable cause to believe that an individual is committing, has committed, or is about to commit a specific offense. 18 U.S.C. § 2518(3)(a). While the two probable cause standards differ, "the differences appear reasonably adapted to the peculiarities of foreign intelligence gathering . . . including the interests of national security that are at stake, the appropriate roles of the executive and the judiciary in the area of foreign policy, and the extraordinary complexities of the field in which the information is to be acquired." *Megahey*, 553 F. Supp. at 1192; *see also Wen*, 477 F.3d at 898 ("[T]he 'probable cause' of which the fourth amendment speaks is not necessarily probable cause to believe that any law is being violated. . . . Probable cause to believe that a foreign agent is communicating with his controllers outside our borders makes an interception reasonable.").

Again, the Court agrees with those courts that have held that FISA does not violate the probable cause requirement of the Fourth Amendment. *See, e.g.*, *Pelton*, 835 F.2d at 1075 (holding FISA "compatible with the Fourth Amendment," despite allowing surveillance on "less than traditional probable cause standard," because "FISA's numerous safeguards provide sufficient protection for the rights guaranteed by the Fourth Amendment"); *Duggan*, 743 F.2d at 74 (concluding FISA requirements "provide an appropriate balance between the individual's interest in privacy and the government's need to obtain foreign intelligence information, and that FISA does not violate the probable cause requirement of the Fourth Amendment."); *see also In re Sealed Case*, 310 F.3d at 739-40, 746. *But see Mayfield*, 504 F. Supp. 2d at 1038-39 (holding

[9] Sections 1805(a)(3) and 1824(a)(3) also provide that no United States person, as defined by § 1801(i), 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.

that FISA violates probable cause requirement of Fourth Amendment).

c. Particularity

Defendants next contend that the government's surveillance did not satisfy the Fourth Amendment particularity requirement because "the duration of these intercepts was not strictly limited." (Mot. to Suppress at 16). Defendants also suggest that FISA-based surveillance fails to satisfy the particularity requirement because of the broad scope of the surveillance. (*Id.* at 17).

FISA orders can be valid for up to 90 days for a U.S. person, as defined by § 1801(i), or up to 120 days for a non-U.S. person. 50 U.S.C. §§ 1805(e), 1824(d). Title III wiretap orders, by contrast, may only last up to 30 days. 18 U.S.C. § 2518(5). Relying on *Berger v. New York*, 388 U.S. 41 (1967), defendants contend that FISA's provisions relating to the duration of surveillance orders do not satisfy Fourth Amendment requirements for criminal investigations and are therefore unreasonable. In *Berger*, the Supreme Court struck down a criminal eavesdropping statute authorizing surveillance for a two-month period on the ground that it violated the particularity requirement. 388 U.S. at 59. The longer periods under FISA, however, are "based on the nature of national security surveillance, which is 'often long range and involves the interrelation of various sources and types of information.'" *In re Sealed Case*, 310 F.3d at 740 (*quoting United States v. United States Dist. Court for the E. Dist. of Mich., S. Div.*, 407 U.S. 297, 322 (1972)). Again, the Court agrees that FISA's order duration provisions do not violate the Fourth Amendment's particularity requirement. *See In re Sealed Case*, 310 F.3d at 740-41, 746.

As for the breadth of the surveillance, FISA requires probable cause to believe that each facility or place under surveillance is being used, or is about to be used, by a foreign power or

agent or the premises to be searched is owned, used, or possessed by an agent of a foreign power. 50 U.S.C. §§ 1805(a)(3)(B), 1824(a)(3)(B). When compared to the Title III warrant requirements, "FISA requires less of a nexus between the facility and the pertinent communications than Title III, but more of a nexus between the target and the pertinent communications." *In re Sealed Case*, 310 F.3d at 740. Accordingly, FISA's particularity requirements, while different from those of Title III, also satisfy the Fourth Amendment. *See id.*; *Cavanagh*, 807 F.2d at 791 ("We reject appellant's suggestion that FISA violates the Fourth Amendment's particularity requirement . . .").

d. Notice

Defendants finally contend that FISA violates the Fourth Amendment's notice requirement because targets need not be notified of the surveillance or search unless fruits of the surveillance or search are to be used in criminal prosecutions.[10] FISA requires only that the government notify an "aggrieved person" against whom the government "intends to enter into evidence or otherwise use or disclose [information obtained or derived from an electronic surveillance or physical search] in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States." 50 U.S.C. §§ 1806(c), 1825(d).

As an initial matter, defendants' standing to challenge the notice provisions of FISA is very much in doubt. Each defendant has received notice that the fruits of FISA surveillance and

[10] Defendants also contend that even FISA targets who receive notice because they are criminally prosecuted have no meaningful opportunity to obtain a remedy for violations of their constitutional rights because they are routinely denied access to the FISA application and order materials. As noted above, the Court has concluded that disclosure is not required in this case.

searches would be used against him, and their challenge accordingly appears to be directed at the rights of others, not their own. *See Ott*, 827 F.2d at 476 (defendant "can argue only that his own statutory rights [under FISA] were violated"); *see generally Rakas v. Illinois*, 439 U.S. 128, 130 n.1 (1978).

In any event, and assuring standing, the Court does not find that the notice requirements of FISA are unreasonable, given the balance of competing interests. As noted, the national security interests at stake differ substantially from traditional criminal surveillance and searches. After considering the legitimate need of the government to gather and safeguard intelligence information, Congress concluded that the need to preserve secrecy for sensitive foreign intelligence information justified eliminating the notice requirement for the subset of situations in which the government would not be utilizing the information in a criminal proceeding. *See* S. Rep. No. 95-701, at 12 (1978) ("The need to preserve secrecy for sensitive counterintelligence sources and methods justifies elimination of the notice requirement."); *Belfield*, 692 F.2d at 145 n.8 ("[N]otice that the surveillance has been conducted, even years after the event, may destroy a valuable intelligence advantage."). Again, the Court agrees with the conclusion of the court in *In re Sealed Case* that FISA's notice provisions are reasonable and do not violate the Fourth Amendment. 310 F.3d at 741-42, 746.

2. FISA's "Significant Purpose" Requirement

Finally, defendants contend that FISA, as amended by the Patriot Act, is unconstitutional because it requires only that a "significant purpose" of FISA surveillance be the procurement of

foreign intelligent information. *See* 50 U.S.C. §§ 1804(a)(7)(B), 1823(a)(7)(B).[11] This issue was thoroughly analyzed by the Foreign Intelligence Surveillance Court of Review in *In re Sealed Case*, 310 F.3d at 736-46. After consideration of the constitutional standards presented in various cases interpreting the Fourth Amendment and FISA, the FISC of Review concluded,

> [e]ven without taking into account the President's inherent constitutional authority to conduct warrantless foreign intelligence surveillance, we think the procedures and government showings required under FISA, if they do not meet the minimum Fourth Amendment warrant standards, certainly come close. We, therefore, believe firmly, applying the balancing test drawn from [*United States v. United States District Court for the Eastern District of Michigan, Southern Division*, 407 U.S. 297 (1972)], that FISA as amended is constitutional because the surveillance [and searches] it authorizes are reasonable.

Id. at 746; *see also Wen*, 477 F.3d at 896; *Holy Land*, 2007 WL 2011319, at *6. *But see Mayfield*, 504 F. Supp. 2d at 1036-42 (criticizing reasoning of *In re Sealed Case* and holding "significant purpose" standard unconstitutional). This Court agrees with that reasoning and accordingly concludes that FISA, as amended by the Patriot Act, does not violate the Fourth Amendment.[12]

The Court further notes that it has reviewed the FISA materials at issue and concludes that all of the surveillance at issue was conducted with an appropriate purpose under the statute—in pre-Patriot Act applications, the government certified that "the purpose" of the surveillance was to obtain foreign intelligence information, and in post-Patriot Act applications,

---

[11] Prior to its October 2001 amendment, FISA had required that "the purpose" of FISA surveillance be the procurement of foreign intelligence information. *In re Sealed Case*, 310 F.3d at 728-29. Several circuits, including the First Circuit, interpreted "the purpose" standard as meaning that the *primary* purpose of the FISA surveillance was procurement of foreign intelligence information. *See, e.g.*, *Johnson*, 952 F.2d at 572; *Pelton*, 835 F.2d at 1075-76; *United States v. Badia*, 827 F.2d 1458, 1464 (11th Cir. 1987).

[12] Even if the statute were deemed unconstitutional, there appears to be no issue as to whether the government proceeded in good faith and in reasonable reliance on the FISA orders. The exclusionary rule would thus not appear to apply under the rule of *United States v. Leon*, 468 U.S. 897 (1984). *See Wen*, 477 F.3d at 897.

the government certified that "a significant purpose" of the surveillance was to obtain foreign intelligence information. In addition, as a practical matter, even for the post-Patriot Act surveillance, the Court is convinced that the primary purpose of the surveillance remained obtaining foreign intelligence information. Therefore, even if this Court were to apply the "primary purpose" standard, as opposed to the "significant purpose" standard, it is satisfied here. *See Hammoud*, 381 F.3d at 334; *Sattar*, 2003 WL 22137012, at *12-13.

Defendant Al-Monla argues that the First Circuit's opinion in *United States v. Johnson*, 952 F.2d at 565, compels a finding that the "significant purpose" amendment to FISA is unconstitutional. In *Johnson*, the court considered the legality of evidence that had been obtained under the pre-amendment version of FISA, and stated the following:

> Although evidence obtained under FISA subsequently may be used in criminal prosecutions, *see* S.Rep. No. 701, 95th Cong., 2d Sess. (1978), *reprinted in* 1978 U.S. Code Cong. & Admin. News 3973, 3979-85 [hereinafter S.Rep. No. 95-701]; *Duggan*, 743 F.2d at 78, the investigation of criminal activity cannot be the primary purpose of the surveillance. *See Duggan*, 743 F.2d at 77; *United States v. Truong Dinh Hung*, 629 F.2d 908, 915 (4th Cir. 1980). The act is not to be used as an end-run around the Fourth Amendment's prohibition of warrantless searches.

Id. at 572. According to defendant, this amounts to a conclusion that any FISA surveillance that does not have the acquisition of foreign intelligence as its "primary purpose" necessarily violates the Fourth Amendment.

This Court disagrees. In context, the phrase "the investigation of criminal activity cannot be the primary purpose of the surveillance" is simply descriptive of the statute as it then existed; it is not a constitutional proscription. Likewise, the sentence that follows ("The act is not to be used as an end-run around the Fourth Amendment's prohibition of warrantless searches") simply describes the purpose and intent of the "primary purpose" requirement. The quoted language

does not, on its face, state a constitutional principle of general application, nor is there any reason to infer one in the context of the opinion. Accordingly, the First Circuit has not spoken to the issue whether the "primary purpose" language was required by the Fourth Amendment, and thus whether the "significant purpose" language of the amended act violates the Constitution. *See In Re Sealed Case*, 310 F.3d at 726-27 (distinguishing *Johnson* on related grounds).

The issues presented in this case—specifically, the need to balance the constitutional protections afforded to citizens under the Fourth Amendment against the imperatives of foreign intelligence gathering—are, to say the least, difficult and complex. Those issues have challenged Congress, the courts, and the executive branch for decades. No solution to the problem is perfect, and all carry substantial costs and burdens. Under the circumstances, this Court cannot conclude that the balance drawn by Congress, and upheld by multiple courts, is unreasonable or otherwise violates the Constitution.

IV. Conclusion

For the foregoing reasons, defendants' motion to compel disclosure of the FISA materials is DENIED, and defendants' alternative motion for *ex parte* review is GRANTED. Defendants' motions to suppress the fruits of the government's FISA-based surveillance and search at issue in this case are DENIED.

So Ordered.

/s/ F. Dennis Saylor
F. Dennis Saylor IV
United States District Judge

Dated: November 5, 2007