

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NORTH CAROLINA
WESTERN DIVISION

NO. 5:09-CR-216-FL

UNITED STATES OF AMERICA

v.

HYSEN SHERIFI;

ANES SUBASIC;

DYLAN BOYD, a/k/a "Mohammed;"

MOHAMMAD OMAR ALY HASSAN;

and

ZIYAD YAGHI,

Defendants.

ORDER

This matter comes before the court on defendants' motions to suppress evidence obtained pursuant to the Foreign Intelligence Surveillance Act ("FISA") and to disclose FISA applications and orders (DE # 680, 805, 816, 818, 812, 810, 813, 841, 843).¹ On May 23, 2011, the government filed public notice on the docket, at entry 1003, of a classified, *ex parte*, omnibus response to the foregoing motions. On June 5, 2011, the government filed its unclassified response on the public docket, lodged at entry 1073. In this posture, the issues raised are ripe for review. For the foregoing reasons, the court denies defendants' motions.

¹ Defendants, for the most part, have moved separately for relief. The court notes that Ziyad Yaghi's ("Yaghi") motions discussed herein are substantively nearly identical to Anes Subasic's ("Subasic"). Mohammed Omar Hassan ("Hassan") incorporates the arguments of his co-defendants. While Hysen Sherifi's ("Sherifi") motion is organized differently, the arguments made are substantively similar. As such, the court addresses all of defendants' motions herein mentioned in omnibus order. Additionally, the government's response notes that it is also a response to Sherifi's motion to compel, lodged on the docket at entry 814. Upon review, the court finds it more appropriate to address that motion when it addresses defendants' pending CIPA § 5 notices, and as such, withholds review of that motion at this time.

STATEMENT OF THE CASE

Defendants are charged in a thirteen (13) count second superseding indictment returned November 24, 2010. Counts one and two allege that beginning no later than November 9, 2006, and continuing through at least July 2009, the eight named co-defendants conspired with each other to provide material support to terrorists in violation of 18 U.S.C. § 2339A, and commit outside of the United States an act that would constitute murder, kidnaping, maiming, and injuring persons in violation of 18 U.S.C. § 956(a). “Violent jihad” and actions taken in furtherance thereof are alleged as overt acts in the conspiracies.

The second superseding indictment charges Daniel Boyd with receiving a firearm through interstate commerce in violation of 18 U.S.C. § 924(b); two counts of possession of a firearm in furtherance of a crime of violence in violation of 18 U.S.C. § 924(c); two counts of knowing sale of a firearm to a convicted felon in violation of 18 U.S.C. § 922(d)(1); two counts of making a false statement in violation of 18 U.S.C. § 1001(a)(2); knowing provision of ammunition to a convicted felon in violation of 18 U.S.C. § 922(d)(1); and conspiracy to kill a federal officer or employee in violation of 18 U.S.C. § 1117. Zakariya Boyd also is charged with two counts of possession of a firearm in furtherance of a crime of violence in violation of 18 U.S.C. § 924(c).²

In addition to the conspiracy charges, Sherifi is charged with two counts of possession of a firearm in furtherance of a crime of violence in violation of 18 U.S.C. § 924(c) and conspiracy to kill a federal officer or employee in violation of 18 U.S.C. § 1117. Dylan Boyd is charged with knowing sale of a firearm to a convicted felon in violation of 18 U.S.C. § 922(d)(1). Counts twelve

² Pursuant to a plea agreement conditionally approved by the court on February 9, 2011 and June 7, 2011, the government agrees to dismiss counts three through eleven against Daniel Boyd and counts two, four, and eight against Zak Boyd.

and thirteen charge that on or about December 2, 2003, Subasic knowingly made false statements while procuring and attempting to procure naturalization, and on his formal application for naturalization, in violation of 18 U.S.C. § 1425(a).³

On July 27, 2009, the government filed seven notices of intent to use FISA information against defendants, lodged on the docket at entries 34 through 40. In their motions, defendants contend that aside from providing this notice, the government has not confirmed any details about what evidence derived from FISA searches and surveillance will be used in the prosecution of the case. Nor has the government provided any affidavits, orders, or other papers which would illustrate for defendants what information was relied upon for the Foreign Intelligence Surveillance Court (“FISC”) to issue orders authorizing any searches or surveillance. Defendants seek various relief, including suppression of all FISA derived evidence, disclosure of FISA derived evidence, and disclosure of FISA applications and orders.

DISCUSSION

A. The Foreign Intelligence Surveillance Act

FISA, enacted in 1978, was Congress’s response to judicial confusion over the existence, nature and scope of a foreign intelligence exception to the Fourth Amendment’s warrant requirement in the wake of the Supreme Court’s 1972 decision in United States v. U.S. District Court, 407 U.S. 297 (1972). See United States v. Rosen, 447 F.Supp.2d 538, 542-543 (E.D.Va. 2006). In addition, FISA was also a response to the Congressional concern over perceived executive branch abuses of such an exception, and the need to provide the executive branch with appropriate means to investigate and counter foreign intelligence threats. Id. FISA establishes a detailed process the

³ Counts twelve and thirteen have been severed for separate trial, pursuant to order entered January 28, 2011, lodged on the docket at entry 750.

executive branch must follow to obtain orders allowing it to collect foreign intelligence information “without violating the rights of citizens of the United States.” United States v. Hammoud, 381 F.3d 316, 332 (4th Cir. 2004) (en banc), vacated on other grounds, 543 U.S. 1097 (2005), reinstated in pertinent part, 405 F.3d 1034 (2005). Although originally limited to electronic surveillance, FISA’s coverage has been expanded to include physical searches as well. See Rosen, 447 F.Supp.2d at 542-43; 50 U.S.C. § 1822.

1. FISA Application

FISA includes a detailed procedure for obtaining orders authorizing electronic surveillance or physical searches of a “foreign power or an agent of a foreign power.” See 50 U.S.C. § 1801. The process begins with the government’s filing of an *ex parte*, under seal application with the FISC. The application must be approved by the Attorney General and must include certain specified information. See Id. §§ 1804(a), 1823(a). A FISC judge considering the application may also require the submission of additional information necessary to make the requisite findings. See id. §§ 1805(a), 1824(a).

The applications for electronic surveillance or physical searches must include the following:

- (1) the identity, if known, or a description of the target of electronic surveillance or physical search;
- (2) a statement of the facts and circumstances relied upon by the applicant to justify the belief that the target is a foreign power or agent of a foreign power and that each of the facilities or places where electronic surveillance is directed or used, or the premises or property subject to physical search are used or are about to be used by a foreign power or agent of a foreign power;
- (3) a statement of the proposed minimization procedures;
- (4) a detailed description of the nature of the information sought and type of surveillance or manner of physical search to be conducted;
- (4) a

certification by an executive branch official; (5) for electronic surveillance, a statement of the means by which the surveillance will be effected, and whether physical entry is required to effect the surveillance; (6) a statement of the facts concerning previous applications and action taken on previous applications; (7) for electronic surveillance, a statement of the period of time for which the surveillance is required to be maintained and if the surveillance should not automatically terminate, a description of facts supporting the belief that additional information will be obtained; and (8) for electronic surveillance, whenever more than one surveillance device is to be used, the coverage of the devices involved and what minimization procedures apply. See id. §§ 1804(a), 1823(a).

2. Certification

Each FISA application must include a certification by an executive officer that includes the following: (1) that the certifying official deems the information sought to be foreign intelligence information;⁴ (2) that a significant purpose of the surveillance or search is to obtain foreign intelligence information; (3) that such information cannot reasonably be obtained by normal investigative techniques; (4) that the type of foreign intelligence information being sought

⁴ FISA defines “foreign intelligence information” 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 or international terrorism 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), 1821(1).

corresponds to the categories describes in section 1801(e) of this title; and (5) includes a statement of the basis for the certification that the information sought is the type of foreign intelligence information designated, and such information cannot reasonably be obtained by normal investigative techniques. See id. §§ 1804(a)(7), 1823(a)(7).

3. Minimization

FISA applications must include a statement of the proposed minimization procedures. Minimization 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 (FISCR 2002). FISA minimization procedures include:

- (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 persons’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.⁵

50 U.S.C. § 1801(h).

Congress intended that the minimization procedures of FISA act as a safeguard for U.S. persons at the acquisition, retention and dissemination phases of electronic surveillance and physical searches. Rosen, 447 F.Supp.2d at 550-51 (citing S. Rep. No. 95-701, at 21-22 (1978), 1978 U.S.C.C.A.N. 3973, 3990-91). Minimization at the acquisition stage is designed to ensure that communications of non-target persons are not improperly disseminated, while minimization at the retention stage is intended to ensure that information acquired that is not necessary for obtaining, producing or disseminating foreign intelligence information is destroyed when feasible. Id.

FISA's minimization procedures are meant to parallel Title III procedures, which courts have construed as not requiring the complete elimination of innocent conversation. Id. Courts, including the Fourth Circuit, have acknowledged the inherent difficulty in determining whether something is related to clandestine activity. The Fourth Circuit has noted that "[a] conversation that seems innocuous on one day may later turn out to be of greater significance, particularly if the individuals involved are talking in code," thus recognizing that it is not always immediately clear whether a particular conversation must be minimized. See Hammoud, 381 F.3d at 334.

⁵ The minimization procedures for physical searches are substantially the same, see 50 U.S.C. § 1821(4), and there is no need to reproduce the language of the statute here. The most significant difference in the language regarding minimization procedures for electronic surveillance and physical search is found in subsection (D) of § 1821(4), which provides that

[N]otwithstanding subparagraphs (A), (B), and (C), with respect to any physical search approved pursuant to section 1822(a) of this title, procedures that require that no information, material, or property of a United States person shall be disclosed, disseminated, or used for any purpose or retained for longer than 72 hours unless a court order under section 1824 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.

§ 1821(4)(D).

FISA requires the Attorney General to adopt minimization procedures. See 50 U.S.C. §§ 1801(h)(1), 1821(4)(A). To fulfill the statutory requirement, the Attorney General has adopted standard minimization procedures that apply to every FISA application. As the government notes, these standard procedures were applied to the applications in the instant case.

4. FISA Order

After review of the application, a judge of the FISC must enter an *ex parte* order granting the government's application for electronic surveillance or physical search of a foreign power or an agent of a foreign power, provided the judge makes certain specific findings, including that on the basis of the facts submitted by the applicant there is probable cause to believe that:

(1) the target of the electronic surveillance or physical search is a foreign power or an agent of a foreign power, *except 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

(2) for electronic surveillance, 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; or

(3) for physical searches, the premises or property to be searched is owned, used, possessed by, or is in transit to or from an agent of a foreign power or a foreign power.

See 50 U.S.C. §§ 1805(a), 1823(a). If the FISC judge finds the government has satisfied the statute's requirements, the judge must issue an *ex parte* order approving the surveillance or search. Id. Such an order must describe the target, the information sought, and the means of acquiring such information. Id. §§ 1805(c)(1), 1824(c)(1). The order must also set forth the period of time during which the electronic surveillance or physical searches are approved, which is generally ninety (90) days or until the objective of the electronic surveillance or physical search has been achieved. Id.

§§ 1805(e)(1), 1824(d)(1). Applications for a renewal of the order must generally be made upon the same basis as the original application and require the same findings by the FISC. Id. §§ 1805(e)(2), 1824(d)(2).

In addition to the probable cause findings, the FISC judge must also find that: (1) that the application has been made by a federal officer and approved by the Attorney General; (2) that the proposed minimization procedures meet the respective definitions of minimization procedures for electronic surveillance and physical searches; and (3) that the application contains all statements and certifications required by 50 U.S.C. § 1804 for electronic surveillance and 50 U.S.C. § 1823 for physical searches and, if the target is a U.S. person, the certification or certifications are not clearly erroneous on the basis of the statement made under sections 1804(a)(7)(E) and 1823(a)(7)(E) of title 18 and any other information furnished under sections 1804(d) and 1823(c) of this title. See id. §§ 1805(a), 1823(a).⁶

5. FISA and Criminal Prosecution

If the Attorney General approves the use of evidence collected pursuant to FISA in a criminal prosecution, and the government intends to use or disclose FISA evidence at the trial of an “aggrieved person,”⁷ the government must first notify the aggrieved person and the district court that the government intends to disclose or use the FISA evidence. See 50 U.S.C. §§ 1806(c), 1825(d).

⁶ Statements “made under sections 1804(a)(7)(E) and 1823(a)(7)(E)” include statements that the information sought is the type of foreign intelligence information designated and that such information cannot reasonably be obtained by normal investigative techniques. See 50 U.S.C. §§ 1804(a)(7)(E), 1823(a)(7)(E).

⁷ An “aggrieved person” under FISA with respect to electronic surveillance is “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). Similarly, with respect 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 subject to physical search.” 50 U.S.C. §§ 1801(k), 1821(2).

On receiving such notification, an aggrieved person may seek to suppress any evidence derived from FISA surveillance or searches on the grounds that: (1) the evidence was unlawfully acquired; or (2) the electronic surveillance or physical search was not conducted in conformity with the order of authorization or approval. *Id.* §§ 1806(e), 1825(f). If an aggrieved person moves to suppress FISA evidence or to obtain FISA material, then upon the filing of an affidavit by the Attorney General stating under oath that disclosure of such material would harm national security, the district court must review the FISA warrant applications and related materials *in camera* and *ex parte* to determine whether the surveillance or search of the aggrieved person was lawfully authorized and conducted. *Id.* §§ 1806(f), 1825(g). The *ex parte, in camera* review is constitutional. *See, e.g., United States v. Benkahla*, 437 F.Supp.2d 541, 554 (E.D.Va. 2006).

The government has notified defendants and the court that it intends to disclose or use FISA evidence in this case. Defendants contend they are aggrieved persons under FISA. Additionally, the government has included an affidavit from the Attorney General stating that public disclosure of the FISA materials or an adversarial hearing with respect to such materials would harm the national security of the United States. (Resp. Ex. 1, ¶ 3.) Accordingly, the court's duty to perform an *ex parte, in camera* review is triggered, and the court has carefully engaged in such a review.

B. Constitutional Challenges to FISA

In challenging the FISA orders and evidence at issue in this case, defendants have raised various constitutional challenges to FISA. Specifically, they argue that the statute, as amended in 2001 by the Providing Appropriate Tools Required to Intercept and Obstruct Terrorism ("PATRIOT") Act, Pub. L. No. 107-56, 115 Stat. 271 (2001), violates the Fourth Amendment.

Prior to the enactment of the PATRIOT Act, the Fourth Circuit recognized that traditional

Fourth Amendment requirements may be relaxed where the “primary” purpose of an investigation is for foreign intelligence purposes. See United States v. Truong Dinh Hung, 629 F.2d 908, 915-16 (4th Cir. 1980). In 2001, Congress amended the language of FISA to indicate that the gathering of foreign intelligence did not have to be the primary purpose of the requested surveillance to obtain a FISA warrant. See United States v. Abu-Jihaad, 630 F.3d 102, 119-20 (2d Cir. 2010). Rather, if all other FISA application requirements were satisfied, the FISC could issue warrants based upon an executive certification that acquisition of foreign intelligence information is a “significant purpose” of the requested surveillance. Id. (citing Pub. L. No. 107-56 § 218, 115 Stat. at 291 (codified as amended at 50 U.S.C. § 1804(a)(6)(B))).

Defendants contend that the PATRIOT Act amendment has unconstitutionally enabled the government to conduct surveillance to gather evidence for use in a criminal case while bypassing traditional warrant requirements as long as the government asserts a significant interest in gathering foreign intelligence. Defendants correctly acknowledge, however, the authorities prevailing against their position. Defendants center much of their argument on the decision in Mayfield v. United States, 504 F.Supp.2d 1023 (D. Ore. 2007), which held that FISA as amended by the PATRIOT Act is unconstitutional. But the Mayfield decision was vacated by the Ninth Circuit on standing grounds. See Mayfield v. United States, 599 F.3d 964, 973 (9th Cir. 2010). Meanwhile, as the government points out, and defendants acknowledge, “all other courts that have considered the [constitutionality of FISA], both before and after enactment of the PATRIOT Act, have rejected constitutional challenges to FISA.” Abu-Jihaad, 630 F.3d 102, 120 (citing multiple cases from various districts around the country); see also In re Sealed Case, 310 F.3d at 735-46; Benkahla, 437 F.Supp.2d at 555 (“Every court, including this one, that has addressed similar [constitutional

challenges to FISA] has completely rejected them.”).⁸

For Fourth Amendment purposes, the “critical question is not whether the executive can certify that obtaining foreign intelligence information is [the] ‘primary’ purpose [of the surveillance], but whether it can certify that it is a *bona fide* purpose of the surveillance.” Abu-Jihaad, 630 F.3d at 128. Congress safeguarded against the possibility of obtaining FISA warrants without a good faith purpose to obtain foreign intelligence information by demanding that in every FISA application a certification that a “significant purpose” of the surveillance or search is to obtain foreign intelligence information. Id. The FISC Court of Review, whose rulings bind the FISA court in issuing surveillance warrants under the statute, has construed the significant purpose test to require “that the government have a measurable foreign intelligence purpose, other than just criminal prosecution of even foreign intelligence crimes.” In re Sealed Case, 310 F.3d at 735. Courts in this circuit have adopted the reasoning of the FISC Court of Review.

Additionally, while the probable cause standard under FISA is different from the standard of Title III,⁹ case law suggests that these differences do not have constitutional implications. See

⁸ The foregoing discussion necessarily forecloses the arguments raised by various defendants regarding the interplay between Katz v. United States, 389 U.S. 347 (1967), Berger v. New York, 388 U.S. 41 (1967), and United States v. United States District Court (Keith), 407 U.S. 297 (1972). While the court has considered the Fourth Amendment arguments presented by this line of cases, this authority does not alter the precedent that holds the FISA amendment under the PATRIOT Act to be constitutional.

⁹ As the court in Rosen noted,

[I]t is important to emphasize the significant difference between FISA’s probable cause requirement and the government’s ultimate burden to prove the existence of criminal activity beyond a reasonable doubt. Indeed, the Fourth Circuit has described probable cause in this context as “a fluid concept-turning on the assessment of probabilities in particular factual contexts-not readily, or even usefully, reduced to a neat set of rules.”

Rosen, 447 F.Supp.2d at 549 (citing Hammoud, 381 F.3d at 332). The court in Rosen noted that in evaluating whether probable cause exists, the court must make a practical, common-sense decision, given all the circumstances set forth in the affidavit, that the search will be fruitful, bearing in mind that under FISA, a judge is permitted to “consider past
(continued...)

In re Sealed Case, 310 F.3d at 738-46. The FISC Court of Review acknowledged that while Title III allows a court to enter an *ex parte* order authorizing electronic surveillance if it determines on the basis of the facts there is probable cause to believe that an individual is committing or is about to commit a crime, FISA, by contrast, requires a showing of probable cause that the target is a foreign power or an agent of a foreign power. Id. at 738. The FISC Court of Review noted that Congress intended a lesser showing of probable cause when activities related to foreign powers or agents of foreign powers are at issue because of the difficulties in surveilling those types of crimes. Id. In particular, the FISC Court of Review found that FISA encompassed the spirit of United States v. United States District Court (Keith), which case recognized that in the context of domestic threats to national security, the focus of security surveillance “may be less precise than that directed against more conventional types of crime.” 407 U.S. 297, 322 (1972). Furthermore, as noted above, the probable cause determination that the target of the electronic surveillance or physical search is a foreign power or an agent of a foreign power, cannot be made solely on the basis “of activities protected by the First Amendment to the Constitution of the United States.” See 50 U.S.C. §§ 1805(a), 1823(a). As such, while defendants correctly point out that FISA provides for a different probable cause standard than Title III, the difference is not unconstitutional.

Defendants offer several more specific arguments as to how FISA violates the Fourth Amendment. These arguments also fail. For instance, arguments that FISA violates the Fourth

⁹(...continued)

activities of the target, as well as facts and circumstances relating to current or future activities of the target.” Id. (citing In re Sealed Case, 310 F.3d at 738). “Thus, while the statute is intended to avoid permitting electronic surveillance solely on the basis of First Amendment activities, it plainly allows a FISC judge to issue an order allowing the surveillance or physical search if there is probable cause to believe that the target, even if engaged in First Amendment activities, may also be involved in unlawful clandestine intelligence activities, or in knowingly aiding and abetting such activities.” Id.

Amendment's requirements of a neutral and detached magistrate, a warrant supported by probable cause, particularity, timely information, and notice, have been rejected by the courts, including courts in this circuit. See, e.g., Abu-Jihaad, 630 F.3d at 123; Hammoud, 381 F.3d at 334; Benkahla, 437 F.Supp.2d 541, 554. As such, the court will not engage in a lengthy discussion regarding these issues.

C. Challenges to Use of FISA-Derived Evidence

1. District Court's De Novo Review

When the district court's *in camera*, *ex parte*, review is prompted by defendants' motions to suppress FISA derived evidence, the review is properly *de novo*. See, e.g., Hammoud, 381 F.3d 316, 332; Rosen, 447 F.Supp.2d at 543-545 ("This review is properly *de novo*, especially given that the review is *ex parte* and thus unaided by the adversarial process.") (citing Hammoud, 381 F.3d at 332). Thus, the court does not give the FISC court's probable cause determinations any deference. Rosen, 447 F.Supp.2d at 545. However, as provided in the FISA statute, the FISA warrant applications are subject to "minimal scrutiny" by the courts, and when the target is a United States person, the court applies the "clearly erroneous" standard to factual averments contained in the certification. 50 U.S.C. §§ 1805(a)(5), 1824(a)(5); Abu-Jihaad, 630 F.3d at 130; see also Rosen, 447 F.Supp.2d at 545 ("[T]he certifications contained in the applications should be 'presumed valid.'"); United States v. Duggan, 743 F.2d 59, 77 n.6 (2d Cir.1984) ("[T]he representations and certifications submitted in support of an application for FISA surveillance should be presumed valid.").

Consistent with these principles, the FISA dockets¹⁰ at issue in this case were reviewed *de novo* with no deference accorded to the FISC's probable cause determinations, but with a presumption of validity accorded to the certifications. See Rosen, 447 F.Supp.2d at 545. Importantly, the review was both searching and conducted with special care, given that the review proceeded *in camera* and *ex parte*, and thus without the full benefit of the adversarial process. Rosen, 447 F.Supp.2d at 545.¹¹ Review of the dockets compels the conclusion that defendants' motions to suppress FISA-derived evidence and to disclose FISA applications and orders must be denied.

Review of the FISA applications, orders and other materials in this case presented none of the concerns raised by defendants that they contend warrant disclosure of the materials or an adversary hearing. The dockets contain the requisite information, outlined above, and review of the dockets revealed that proper minimization procedures were established and followed. Any failure to minimize was inadvertent, disclosed to the FISC on discovery, and promptly rectified.

The court carefully reviewed the dockets, keeping in mind the concerns defendants have raised with regard to the *ex parte*, *in camera* nature of the proceedings and the findings of probable cause. The court gave particular attention to issues of probable cause and the facts alleged in the applications before examining the orders themselves. The court is satisfied that probable cause existed that the targets of surveillance or physical searches were foreign powers or agents of a foreign power, that this finding was not based solely on the basis of activities protected by the First

¹⁰ The term "FISA docket" as used herein refers to all the materials required for a FISA application as well as the order that issued from the FISC court, and any returns filed in connection with the order.

¹¹ Although defendants did not have access to the FISA material, and thus were not able to present arguments concerning specific materials, they nonetheless participated in the review process through the submission of thoroughly researched memorandum of law based on publicly available information regarding FISA. See Rosen, 447 F.Supp.2d at 545.

Amendment, and that the facilities to be surveilled and property to be searched were owned, used, possessed by, or were in transit to or from an agent of a foreign power.¹² Lastly, the affidavits or certifications submitted as part of the FISA applications were not clearly erroneous within the meaning of 50 U.S.C. §§ 1805(a)(5) and 1824 (a)(5). As such, defendant's motions are denied, and the FISA materials will not be disclosed. An adversary hearing is not required.

CONCLUSION

For the foregoing reasons, defendants' motions to suppress evidence obtained pursuant to the Foreign Intelligence Surveillance Act ("FISA") and to disclose FISA applications and orders (DE # 680, 805, 816, 818, 812, 810, 813, 841, 843) are DENIED.

SO ORDERED, this the 22nd day of June, 2011.

A handwritten signature in black ink, reading "Louise W. Flanagan". The signature is written in a cursive, flowing style. Below the signature is a horizontal line.

LOUISE W. FLANAGAN
Chief United States District Judge

¹² Because the court finds probable cause existed for the FISA orders at issue, it does not address the government's argument regarding the good faith exception to the exclusionary rule.