

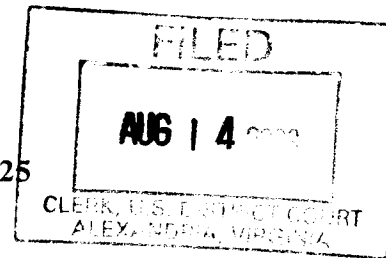
UNCLASSIFIED

FILED WITH THE
COURT SECURITY OFFICER
CSO: [Signature]
DATE: 8/14/2006

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

UNITED STATES OF AMERICA,)
)
 v.)
)
 STEVEN J. ROSEN)
 KEITH WEISSMAN)

Case No. 1:05cr225



MEMORANDUM OPINION

Defendants, Steven J. Rosen and Keith Weissman, are charged in a superseding indictment with one count of conspiring to communicate national defense information to persons not entitled to receive it, in violation of 18 U.S.C. § 793(d), (e) and (g). More specifically, Count One of the superseding indictment, which spans twelve pages and includes fifty-seven overt acts, alleges that between April 1999 and continuing until August 2004, Rosen and Weissman along with alleged co-conspirator Lawrence Franklin, then an employee of the Department of Defense (“DOD”), were engaged in a conspiracy to communicate information relating to the national defense to those not entitled to receive it. According to the superseding indictment, Franklin and certain other unnamed government officials with authorized possession of classified national defense information communicated that information to Rosen and Weissman, who were employed at the time as lobbyists for the American-Israel Public Affairs Committee (AIPAC). It is further alleged that Rosen and Weissman then communicated the information received from their government sources to members of the media, other foreign policy analysts, and certain foreign officials, none of whom were authorized to receive this information.

UNCLASSIFIED

#343

In addition, the superseding indictment also charges defendant Rosen with one count of aiding and abetting the communication of national defense information to persons not entitled to receive it, in violation of 18 U.S.C. §§ 793(d) and 2. This count alleges that Rosen aided and abetted Franklin's violation of 18 U.S.C. § 793(d) by providing a fax number to Franklin so that Franklin could fax to Rosen a document Franklin had prepared containing national defense information derived from a classified document.

In the course of its investigation of the alleged conspiracy, the government sought and obtained orders issued by the Foreign Intelligence Surveillance Court ("FISC") pursuant to the Foreign Intelligence Surveillance Act ("FISA"), 50 U.S.C. § 1801 *et seq.*, authorizing certain physical searches and electronic surveillance. As the investigation pertained to national security, these applications and orders were classified. Because the government intends to offer evidence obtained or derived from physical searches and electronic surveillance authorized by these orders, defendants seek by motion (1) to obtain disclosure of the classified applications submitted to the FISC, the FISC's orders, and related materials, and/or (2) to suppress the evidence obtained or derived from any searches or surveillance conducted pursuant to the issued FISA orders. In response to defendants' motion the government filed: (1) a classified, *ex parte* brief in opposition to the defendants' motion; (2) an unclassified, redacted brief in opposition to the defendants' motion; (3) a declaration and claim of privilege of the Attorney General of the United States; (4) a classified Declaration of an Assistant Director of the Federal Bureau of Investigation ("FBI") concerning the classified minimization procedures; and (6) certified copies of the FISA applications, orders and related materials at issue in this case.

Defendants' motion and the government's opposition raise a number of questions

concerning the proper scope of, and procedure for, district court review of challenges to FISA orders, as well as specific questions concerning whether the FISA orders in issue in this case issued in conformity with that statute's requirements. This memorandum opinion addresses these questions, beginning with an overview of the FISA procedure.

I.

FISA, enacted in 1978, was Congress's response to three related concerns: (1) the judicial confusion over the existence, nature and scope of a foreign intelligence exception to the Fourth Amendment's warrant requirement that arose in the wake of the Supreme Court's 1972 decision in *United States v. United States District Court*, 407 U.S. 297 (1972);¹ (2) the Congressional concern over perceived Executive Branch abuses of such an exception;² and (3) the felt need to provide the Executive Branch with an appropriate means to investigate and counter foreign intelligence threats.³ FISA accommodates these concerns by establishing a detailed process the Executive Branch must follow to obtain orders allowing it to collect foreign intelligence

¹*Compare Zweibon v. Mitchell*, 516 F.2d 594, 613-14 (D.C.Cir. 1975) (plurality opinion) (“Although we believe that an analysis of the policies implicated by foreign intelligence surveillance indicates that, absent exigent circumstances, all warrantless electronic surveillance is unreasonable and therefore unconstitutional, our holding need not sweep that broadly.”) *with United States v. Brown*, 484 F.2d 418, 426-27 (5th Cir. 1973) (President's authority to conduct foreign affairs includes ability to conduct foreign intelligence surveillance without a warrant); *United States v. Butenko*, 494 F.2d 593, 605 (3d Cir. 1974) (en banc) (same). The Fourth Circuit, in a post-FISA decision regarding pre-FISA surveillance, held that the executive may conduct warrantless surveillance if the “primary purpose” is collecting foreign intelligence information. See *United States v. Truong Dinh Hung*, 629 F.2d 908, 915-16 (4th Cir. 1980).

²See S.Rep.No. 95-604(I), at 7, 1978 U.S.C.A.N. 3904, 3908 [Hereinafter S. Judiciary Comm. Rep.] (“This legislation is in large measure a response to the revelations that warrantless electronic surveillance in the name of national security has been seriously abused.”).

³See generally William C. Banks and M.E. Bowman, *Executive Authority for National Security Surveillance*, 50 Am. U. L. Rev. 1, 75-76 (2000) (describing the impetus for FISA).

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 now been expanded to include physical searches, as well. Thus, the detailed FISA process applicable to electronic surveillance relating to foreign intelligence also applies now to physical searches.⁴

FISA’s detailed procedure for obtaining orders authorizing electronic surveillance or physical searches of a foreign power or an agent of a foreign power begins with the government’s filing of an *ex parte*, under seal application with the FISC.⁵ Such an application must be approved by the Attorney General and must include certain specified information. *See* 50 U.S.C. §§ 1804(a) and 1823(a). A FISC judge considering the application may also require the submission of additional information necessary to make the requisite findings under §§ 1805(a) and 1824(a).

After review of the application, a single judge of the FISC must enter an *ex parte* Order

⁴*See* Intelligence Authorization Act for Fiscal Year 1995, Pub. L. No. 103-359, 108 Stat. 3443 (1994) (codified as amended at 50 U.S.C. § 1821 *et seq.*). And, in 1998, Congress further amended FISA to create slightly different procedures for authorizing the use of pen registers and trap and trace devices for foreign intelligence information, *see* Intelligence Authorization Act for Fiscal Year 1999, Pub. L. No. 105-272, 112 Stat. 2405 (1998) (codified as amended at 50 U.S.C. § 1841 *et seq.*), and to allow the executive branch access to business records for foreign intelligence and international terrorism investigations. *See* 18 U.S.C. §§ 1861-63. The parties’ dispute involves only electronic surveillance and physical searches conducted pursuant to FISA.

⁵The FISC consists of eleven district court judges selected by the Chief Justice from at least seven judicial circuits and serving staggered seven year terms. *See* 50 U.S.C. § 1803(a). At least three of the FISC’s judges must reside within twenty miles of Washington, D.C. *Id.* In the unlikely event that a FISA application is denied by a judge of the FISC, the government may seek review of such denial in the Foreign Intelligence Surveillance Court of Review (FISCR), and if necessary, in the Supreme Court of the United States. *See* 50 U.S.C. § 1803(b).

granting the government's application for electronic surveillance or a physical search of a foreign power or an agent of a foreign power provided the judge makes certain specific findings, including most importantly, 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) and 1823(a).⁶ If the FISC judge's findings reflect that the government has satisfied the statute's requirements, the judge must issue an order approving the surveillance or search. Such an order must describe the target, the information sought, and the means of acquiring such information. *See* 50 U.S.C. §§ 1805(c)(1) and 1824(c)(1). The order must also

⁶In addition to these probable cause findings, the FISC judge must also find that: (1) the President has authorized the Attorney General to approve applications for electronic surveillance or physical searches for foreign intelligence information; (2) that the application has been made by a Federal officer and approved by the Attorney General; (3) that the proposed minimization procedures meet the respective definitions of minimization procedures for electronic surveillance and physical searches; and (4) 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 United States 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* 50 U.S.C. §§ 1805(a) and 1823(a).

set forth the period of time during which the electronic surveillance or physical searches are approved, which is generally ninety days or until the objective of the electronic surveillance or physical search has been achieved. *See* 50 U.S.C. §§ 1805(e)(1) and 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. *See* 50 U.S.C. §§ 1805(e)(2) and 1824(d)(2).

Although FISA is chiefly directed to obtaining “foreign intelligence information,”⁷ the Act specifically contemplates cooperation between federal authorities conducting electronic surveillance and physical searches pursuant to FISA and federal law enforcement officers investigating clandestine intelligence activities. In this respect, FISA explicitly allows the use of evidence derived from FISA surveillance and searches in criminal prosecutions. *See* 50 U.S.C. §§ 1806(k) and 1825(k).

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

⁷FISA 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).

an “aggrieved person,”⁸ 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) and 1825(d). 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. *See* 50 U.S.C. §§ 1806(e) and 1825(f). And, 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.” 50 U.S.C. §§ 1806(f) and 1825(g).

This review is properly *de novo*, especially given that the review is *ex parte* and thus unaided by the adversarial process. *See United States v. Hammoud*, 381 F.3d 316, 332 (4th Cir. 2004) (en banc) (conducting *de novo* review of FISA materials); *United States v. Squillacote*, 221 F.3d 542, 554 (4th Cir. 2000) (same). Thus, the government’s contention here that a reviewing district court must accord the FISC’s probable cause determination “substantial deference” cannot be sustained in light of the Fourth Circuit’s clear contrary statement on the issue.

⁸FISA defines an “aggrieved person” with respect to electronic surveillance as “a person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance.” 50 U.S.C. § 1801(k). With respect to physical searches, FISA similarly defines an “aggrieved person” as 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. § 1821(2).

Hammoud, 381 F.3d at 332 (“Having conducted our own *de novo* review of the materials we reach the same conclusion as the magistrate judge and the district court.”) (citing *Squillacote*, 221 F.3d at 554). But the government is correct that the certifications contained in the applications should be “presumed valid.” See 50 U.S.C. § 1805(a)(5) (applying “clearly erroneous” standard to factual averments contained in certification when the target is a United States person); *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 dockets⁹ 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. Importantly, the review was both searching and conducted with special care, given that the review proceeded *in camera* and *ex parte* and hence without the full benefit of the adversarial process.¹⁰

II.

At the threshold, defendants seek disclosure of the FISA applications, orders, and related materials at issue in this case so they may effectively participate in the review process. On this point FISA is clear: It allows a reviewing court to disclose such materials “only where such

⁹The term “docket” as used here refers to all the pleadings, affidavits, and other papers required for a FISA application, as well as the order that issued as a result and any returns filed in connection with the order.

¹⁰Although 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 memorandum of law based on publicly available information and setting forth their general legal propositions.

disclosure is necessary to make an accurate determination of the legality of the surveillance.” 50 U.S.C. § 1806(f). Defendants claim this condition is met, by arguing (1) that the FISC’s determination that they were agents of a foreign power was surely wrong; and (2) that evidence of the government’s evident failure to comply with FISA’s minimization procedures requires disclosure. Neither argument is persuasive.

As the Fourth Circuit has made clear, an *ex parte* and *in camera* review is the standard means for assessing the legality of surveillance conducted pursuant to FISA, and disclosure should occur—

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

United States v. Belfield, 692 F.2d 141, 147 (4th Cir. 1982) (quoting S. Intelligence Rep. at 64).

The exceptional nature of disclosure of FISA material is especially appropriate in light of the possibility that such disclosure might compromise the ability of the United States to gather foreign intelligence effectively. *See Id.*

Indeed, no court in this circuit to consider a motion to suppress pursuant to § 1806(f) has found it necessary to disclose the FISA materials in order to make a facial determination of legality. *See, e.g., United States v. Squillacote*, 221 F.3d 542, 553-54 (4th Cir. 2000); *In re Grand Jury Proceedings*, 856 F.2d 685, 688 n.3 (4th Cir. 1988); *United States v. Nicholson*, 955 F.Supp. 588, 592 & n.11 (E.D.Va. 1997) (“this court knows of no instance in which a court has required an adversary hearing or disclosure in determining the legality of a FISA surveillance.”).

This is also consistent with the practice of other circuits to have considered the issue. *See, e.g., United States v. Dumeisi*, 424 F.3d 566, 578-79 (7th Cir. 2005); *United States v. Damrah*, 412 F.3d 618, 624 (6th Cir. 2005); *United States v. Johnson*, 952 F.2d 565, 571-72 (1st Cir. 1991).

Review of the FISA applications, orders and other materials in this case presented none of the concerns that might warrant disclosure to defendants. The FISA dockets contained no facial inconsistencies, nor did they disclose any reason to doubt any of the representations made by the government in its applications. Likewise, the targets of the surveillance are precisely defined. Finally, although defendants claim that the discovery obtained from the government contains a significant amount of non-foreign intelligence information, this contention relies upon an inordinately narrow view of what constitutes foreign intelligence information, and therefore is unavailing.¹¹ For these reasons, and given the government's legitimate national security interest in maintaining the secrecy of the information contained in the FISA applications, disclosure of the FISA materials to defendants is not warranted in this case.

III.

It is next necessary to address the lawfulness of the FISC's authorization of the electronic surveillance and physical searches conducted by the government in this case. In this regard, a careful and searching review of the FISA dockets discloses that the government's applications and the resulting FISC orders meet all the statutory requirements. Specifically, the President has authorized the Attorney General to approve applications to the FISC and each of the applications reviewed was made by a federal officer and approved by the Attorney General or his authorized designate. In addition, (i) the proposed minimization procedures met the statutory requirements

¹¹*See infra* Part III.

contained in § 1801(h), (ii) the applications contained all of the required statements and certifications, and (iii) those certifications were not clearly erroneous on the basis of the facts submitted pursuant to § 1804(a)(7)(E). *See* 18 U.S.C. § 1805(a).

Defendants' attack on the lawfulness of the FISA surveillance in this case focuses chiefly on two issues: (1) whether the FISC had probable cause to believe that the targets of the sanctioned surveillance were "agents of a foreign power," as required by FISA, and (2) whether there was proper compliance with the minimization procedures subsequent to the surveillance. Review of the FISA material confirms that both of these issues must be resolved in favor of the lawfulness of the surveillance.

Defendants' necessarily speculative contention that the FISC must have erred when it found probable cause to believe that the targets are agents of a foreign power is without merit. An agent of a foreign power is defined by the statute, in pertinent part, as any person who—

(A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States;

(B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such power, which activities involve or are about to involve a violation of the criminal statutes of the United States;

...
or

(E) knowingly aids or abets any person in the conduct of activities described in [the subparagraphs above] or knowingly conspires with any person to engage in activities described in [the subparagraphs above].

50 U.S.C. § 1801(b)(2). Although the phrase "clandestine intelligence gathering activities" is not defined in FISA, the legislative history demonstrates that the drafters viewed these "activities" in light of the criminal espionage laws, including 18 U.S.C. §§ 793 and 794, and considered that

such “activities” would include, for example, “collection or transmission of information or material that is not generally available to the public.” *See* S. Rep. No. 95-701, at 21-22 (1978), 1978 U.S.C.C.A.N. 3973, 3990-91) [Hereinafter S. Intelligence Rep.].¹² In addition, with respect to paragraph (E) above, Congress added “knowingly” to ensure that “the aider or abettor cannot be an unknowing dupe. The bill requires that he know that the person he is aiding is engaged in the described activities.” S. Judiciary Comm. Rep. at 17-18.

Importantly, FISA is clear that in determining whether there is probable cause to believe that a potential target of FISA surveillance or a FISA search is an agent of a foreign power, the FISC judge may not consider a United States person an agent of a foreign power “*solely* upon the basis of activities protected by the First Amendment.” 50 U.S.C. § 1805(a) (emphasis added). From this plain language,¹³ it follows that the probable cause determination may rely in part on activities protected by the First Amendment, provided the determination also relies on activities not protected by the First Amendment. This issue received extensive treatment in the legislative

¹²The Senate Intelligence Report states:

The agent must also be knowingly engaged in ‘clandestine intelligence gathering activities’ that involve or may involve violations of federal criminal law. It is anticipated that most of the persons under surveillance under this subparagraph will be violating the criminal espionage laws which appear in Title 18, U.S.C. §§ 792-99, 951; Title 42, U.S.C. §§ 2272-2278B; and Title 50, U.S.C. § 855.

Id. at 21.

¹³A statute’s plain meaning should be ignored “only in those rare instances in which there is a clearly expressed legislative intent to the contrary, in which a literal application of the statute would thwart its obvious purpose, or in which a literal application of the statute would produce an absurd result.” *See Chesapeake Ranch Water Co. v. Board of Comm’rs of Calvert County*, 401 F.3d 274, 280 (4th Cir. 2005) (quoting *Holland v. Big River Minerals Corp.*, 181 F.3d 597, 603 n.2 (4th Cir. 1999)).

history, which, consistent with the statute's plain language, makes clear that First Amendment activities cannot form the *sole* basis for concluding a U.S. person is an agent of a foreign power.

The following excerpt from the legislative history illustrates this point:

The Bill is not intended to authorize electronic surveillance when a United States person's activities, even though secret and conducted for a foreign power, consist entirely of lawful acts such as lobbying or the use of confidential contacts to influence public officials, directly or indirectly, through the dissemination of information. Individuals exercising their right to lobby public officials or to engage in political dissent from official policy may well be in contact with representatives of foreign governments and groups when the issues concern foreign affairs or international economic matters.

They must continue to be free to communicate about such issues and to obtain information or exchange views with representatives of foreign governments or with foreign groups, free from any fear that such contact might be the basis for probable cause to believe they are acting at the direction of a foreign power thus triggering the government's power to conduct electronic surveillance.

See S. Intelligence Rep. at 29.

The legislative history makes equally clear, however, that this protection extends only to the "*lawful* exercise of First Amendment rights of speech, petition, assembly and association."

Id. (emphasis added). Similarly, the House Report (Intelligence Committee) emphasized that FISA "would not authorize surveillance of ethnic Americans who *lawfully* gather political information and perhaps even *lawfully* share it with the foreign government of their national origin." *See In re Sealed Case*, 310 F.3d 717, 739 (FISCR 2002) (emphasis added) (quoting H. Rep. No. 95-1283, at 40). For example, electronic surveillance might be appropriate if there is probable cause to believe that—

foreign intelligence services [are] hid[ing] behind the cover of some person or organization in order to influence American political events and deceive Americans into believing that the opinions or influence are of domestic origin and initiative and such deception is willfully maintained in violation of the Foreign Agents Registration Act.

S. Intelligence Rep. at 29. Thus, if the FISC judge has probable cause to believe that the potential target is engaged in *unlawful* activities in addition to those protected by the First Amendment, the FISC may authorize surveillance of a U.S. person. See *In re Sealed Case*, 310 F.3d at 738 (“We have noted, however, that where a U.S. person is involved, an ‘agent of a foreign power’ is defined in terms of criminal activity.”).

In this respect, it 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.” *United States v. Hammoud*, 381 F.3d at 332 (upholding probable cause finding that Hammoud was an agent of Hizballah). Furthermore, “[i]n evaluating whether probable cause exists, it is the task of the issuing judge ‘to make a practical, common-sense decision, whether, given all the circumstances set forth in the affidavit, there is a fair probability’ that the search will be fruitful.” *Id.* (quoting *Illinois v. Gates*, 462 U.S. 213, 238 (1983)); See also *Mason v. Godinez*, 47 F.3d 852, 855 (7th Cir. 1995) (“Probable cause means more than bare suspicion but less than absolute certainty that a search will be fruitful.”). And, in making the probable cause determination, FISA permits a judge to “consider past activities of the target, as well as facts and circumstances relating to current or future activities of the target.” 50 U.S.C. § 1805(b). Furthermore, with respect to those U.S. persons suspected of involvement in clandestine intelligence activities, the probable cause determination “does not necessarily require a showing of an imminent violation of criminal law” because “Congress clearly intended a lesser showing of probable cause for these activities

than that applicable to ordinary cases.” *In re Sealed Case*, 310 F.3d at 738. Illustrative of this intent is FISA’s description of clandestine intelligence activities as those that “involve or *may* involve a violation of the criminal statutes of the United States.” 50 U.S.C. § 1801(b)(2)(A); *see In re Sealed Case*, 310 F.3d at 738. As FISA’s drafters made clear: “The term ‘may involve’ not only requires less information regarding the crime involved, but also permits electronic surveillance at some point prior to the time when a crime sought to be prevented, as for example, the transfer of classified documents, actually occurs.” *In re Sealed Case*, 310 F.3d at 738 (quoting H. Rep. No. 95-1283, at 40). 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. In these circumstances, the fact that a target is also involved in protected First Amendment activities is no bar to electronic surveillance pursuant to FISA.¹⁴

A thorough review of the FISA dockets in issue confirms that the FISC had ample probable cause to believe that the targets were agents of a foreign power quite apart from their First Amendment lobbying activities. While the defendants’ lobbying activities are generally

¹⁴*See United States v. Dumeisi*, 424 F.3d 566, 579 (7th Cir. 2005) (“We have reviewed the classified materials relied upon by the FISC and conclude that the government provided probable cause that Dumeisi was an agent of a foreign power entirely independent of any of his journalistic activities.”). *See also United States v. Sattar*, 2003 WL 22137012, at *8 (S.D.N.Y. 2003) (denying that the probable cause determination was “based on communications regarding [defendant’s] views about the conditions and government in Egypt that are protected by the First Amendment.”); *Global Relief Foundation, Inc. v. O’Neill*, 207 F.Supp.2d 779, 790 (N.D.Ill. 2002); *United States v. Rahman*, 861 F.Supp. 247, 252 (S.D.N.Y. 1994).

protected by the First Amendment, willful violations of § 793 are not, and as is demonstrated by the allegations contained in the superseding indictment, the FISC had probable cause to believe that such violations had occurred in this case. *See United States v. Rosen*, ___ F.Supp.2d ___, Case No. 1:05cr225 (E.D.Va. August 9, 2006) (memorandum opinion denying the defendants' motion to dismiss the superseding indictment for violation of the First Amendment's guarantee of free speech).

Defendants' second argument in support of their motion is that the government failed to follow the applicable minimization procedures. In this regard, it is true that once the electronic surveillance or the physical search has been approved, the government must apply the specific minimization procedures contained in the application to the FISC. These 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). While the specific minimization procedures for each application are classified, they must meet the definition of minimization procedures under § 1801(h) for electronic surveillance and § 1821(4) for physical searches. FISA minimization procedures include, in pertinent part—

- (1) specific procedures adopted by the Attorney General that are reasonably designed in light of the purpose and technique of the particular surveillance or search, 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, 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.

See 50 U.S.C. §§ 1801(h) and 1821(4). Congress intended these minimization procedures to act as a safeguard for U.S. persons at the acquisition, retention and dissemination phases of electronic surveillance and searches. *See* S. Intelligence Rep. at 39. Thus, for example, minimization at the acquisition stage is designed to insure that the communications of non-target U.S. persons who happen to be using a FISA target's telephone, or who happen to converse with the target about non-foreign intelligence information, are not improperly disseminated. *See id.* Similarly, minimization at the retention stage is intended to ensure that "information acquired, which is not necessary for obtaining, producing, or disseminating foreign intelligence information, be destroyed where feasible." *See In re Sealed Case*, 310 F.3d at 731 (quoting H. Rep. No. 95-1283, at 56). Finally, the dissemination of foreign intelligence information "needed for an approved purpose . . . should be restricted to those officials with a need for such information." *Id.* As the Foreign Intelligence Surveillance Court of Review has recently made clear, these procedures do not prohibit the sharing of foreign intelligence information between FBI intelligence officials and criminal prosecutors when there is evidence of a crime. *Id.*

FISA's minimization procedures are meant to parallel the minimization procedures of Title III, which courts have sensibly construed as not requiring the total elimination of innocent conversation. *See* S. Intelligence Rep. at 39 (citing *United States v. Bynum*, 485 F.2d 490, 500

(2d Cir. 1973), *cert. denied* 423 U.S. 1005 (1975)).¹⁵ On the contrary, “[i]n assessing the minimization effort, the Court’s role is to determine whether ‘on the whole the agents have shown a high regard for the right of privacy and have done all they reasonably could to avoid unnecessary intrusion.’” *Id.* at 39-40 (quoting *United States v. Tortorello*, 480 F.2d 764 (2d Cir.), *cert. denied* 414 U.S. 886 (1973)). Thus, “[a]bsent a charge that the minimization procedures have been disregarded completely, the test of compliance is ‘whether a good faith effort to minimize was attempted.’” *Id.* (quoting *United States v. Armocida*, 515 F.2d 29, 44 (3d Cir. 1975)).

Obviously, the extent of the government’s minimization will depend largely on its construction of the term “foreign intelligence information.”¹⁶ And in this respect, “foreign intelligence information” includes, among other things, “information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against . . . clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power.” 50 U.S.C. § 1801(e). Acknowledging the inherent difficulty in determining whether something is related to clandestine activity, courts have construed “foreign intelligence information” broadly and sensibly allowed the government some

¹⁵Title III’s minimization procedures provide, in pertinent part, that:

Every order and extension thereof shall contain a provision that the authorization to intercept shall be executed as soon as practicable, shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter, and must terminate upon attainment of the authorized objective, or in any event in thirty days.

See 18 U.S.C. § 2518(5).

¹⁶*See supra* note 9.

latitude in its determination of what is foreign intelligence information. As the Fourth Circuit pointed out, “[i]t is not always immediately clear” whether a particular conversation must be minimized because “[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.” *Hammoud*, 381 F.3d at 334. For this reason, “when the government eavesdrops on clandestine groups . . . investigators often find it necessary to intercept all calls in order to record possible code language or oblique references to the illegal scheme.” *United States v. Truong*, 629 F.2d 908, 917 (4th Cir. 1980).¹⁷ This latitude was intended by FISA’s drafters who understood that it may be necessary to “acquire, retain and disseminate information concerning . . . the known contacts” of a U.S. person engaged in clandestine intelligence activities even though some of those contacts will invariably be innocent of any wrong-doing. H. Rep. No. 95-1283, at 58.

Given the breadth of the term “foreign intelligence information” in the context of investigating clandestine intelligence activities and the rule of reason that applies to the government’s obligation to minimize non-pertinent information, defendants’ motion to suppress for failure to properly minimize must be denied. The *ex parte, in camera* review of the FISA

¹⁷See also *United States v. Hoffman*, 832 F.2d 1299, 1308 (1st Cir.1987) (“Where, as here, an investigation is focused largely on blueprinting the shape of the conspiratorial wheel and identifying the spokes radiating from its hub, the need to allow latitude to eavesdroppers is close to its zenith.”); *United States v. Bin Laden*, 126 F.Supp. 2d 264, 286 (S.D.N.Y. 2000) (allowing “more extensive monitoring” and “greater leeway” to determine scope of conspiracy); *Halperin v. Kissinger*, 723 F.Supp. 1535, 1548 (D.D.C. 1989) (“The monitor’s ability to minimize nonpertinent calls becomes even more difficult when the wiretap is prompted by numerous leaks of highly sensitive foreign policy and military information. In that situation, the monitor – who normally would not be privy to such closely held policies and initiatives – often would not have the background and experience to distinguish with precision between a leak of insider information and an expression of opinion on a matter of topical concern (such as SALT or Vietnam).”).

dockets discloses that any failures to minimize properly the electronic surveillance of the defendants were (i) inadvertent, (ii) disclosed to the FISC on discovery, and (iii) promptly rectified.

Yet, this does not end the analysis as the defendants also point to certain publicly available materials bearing on the FBI's general compliance with FISA during the period of this investigation. Specifically, defendants refer to (1) certain previously classified FBI documents, obtained by the media via the Freedom of Information Act, 5 U.S.C. § 552, detailing violations of minimization procedures in certain unrelated cases, and (2) a March 8, 2006 Department of Justice, Office of the Inspector General Report to Congress on Implementation of Section 1001 of the USA Patriot Act describing certain failures of the FBI to adhere to FISA's requirements. These documents are general assessments and do not specifically address the integrity of the minimization effort that occurred here. As such, they are no more probative of a failure of minimization in this case than a general study of errors committed over a period of years in baseball would be probative of whether errors occurred in a specific game.

No doubt anticipating this, defendants also cite pre-indictment media reports of the charges eventually brought against Rosen, Weissman and alleged co-conspirator Franklin. In defendants' view these media reports are evidence of an intentional disregard for minimization requirements because the information in these reports could only have come from FISA surveillance. Specifically, defendants cite the following media reports:¹⁸

1. A CBS Evening News broadcast on August 27, 2004, that informed its viewers that “a

¹⁸These media reports also form part of the basis of defendants' pending motion seeking a show cause hearing, dismissal of the indictment, and imposition of sanctions based on a violation of Rule 6(e), Fed.R.Crim.P., which motion is under advisement and will be resolved separately.

suspected spy” at DOD had turned over classified information, including information relating to a draft “presidential directive on U.S. policy towards Iran” to two AIPAC employees who delivered the information to the Government of Israel. *See FBI Probes Pentagon Spy*, CBS Evening News television broadcast, August 27, 2004. *See also Pentagon Mole Probe*, CBS Evening News television broadcast, August 30, 2004 (identifying Franklin as the “suspected spy”).

2. A September 1, 2004 New York Times article identifying the two AIPAC officials as defendants Rosen and Weissman, but only after a lawyer hired by AIPAC publicly confirmed that the F.B.I. had interviewed the two men. *See David Johnston, FBI Interviews 2 Suspected of Passing Secrets to Israel*, N.Y. Times, September 1, 2004 at A15.
3. A September 2, 2004 Miami Herald news brief identifying Rosen and Weissman as the focus of “an F.B.I. investigation into whether a Pentagon employee provided them with classified material about Iran that was passed on to Israel.” *See National Briefs*, Miami Herald, September 2, 2004 at 5A.

Even assuming these media reports came from a FISA minimization breach – other plausible explanations exist – a single unauthorized leak does not establish a complete disregard of the minimization requirements sufficient to warrant suppression of the entire investigation. FISA’s minimization requirements were designed to protect the privacy interests of FISA targets, but these requirements are subject to a rule of reason and were not intended to invest a rogue official with the power to undermine a lengthy investigation. This sensible point was well-

recognized by FISA's drafters who found persuasive the analogous Title III case law.¹⁹

Accordingly, these news reports do not suffice on this record to warrant suppression of the FISA surveillance and an appropriate order will enter. This order will also grant defendants leave to renew this motion on this ground alone should the results of an investigation of the leak, which will be separately ordered, warrant doing so.

An appropriate order will issue.

Alexandria, Virginia
August 14, 2006

/s/
T.S. Ellis, III
United States District Judge

¹⁹See S. Intelligence Rep. at 39 ("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.'") (quoting *United States v. Armocida*, 515 F.2d 29, 44 (3d Cir. 1975)). See also *In re Sealed Case*, 310 F.3d 717, 731 (2002) ("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.") (emphasis added).