

**UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA**

UNITED STATES OF AMERICA,

Criminal No. 04-29 (JRT)

Plaintiff,

v.

MOHAMED ABDULLAH WARSAME,

**MEMORANDUM OPINION AND
ORDER DENYING DEFENDANT'S
MOTION FOR DISCLOSURE AND
MOTION TO SUPPRESS**

Defendant.

Thomas M. Hollenhorst, Assistant United States Attorney, **OFFICE OF THE UNITED STATES ATTORNEY**, 600 United States Courthouse, 300 South Fourth Street, Minneapolis, MN 55415; and Joseph N. Kaster, **UNITED STATES DEPARTMENT OF JUSTICE**, 10th and Constitution Avenue NW, Room 2649, Washington, DC 20530, for plaintiff.

David C. Thomas, **LAW OFFICES OF DAVID C. THOMAS**, 53 West Jackson Boulevard, Suite 1362, Chicago, IL 60604; and Andrea K. George, **FEDERAL PUBLIC DEFENDER**, 300 South Fourth Street, Suite 107, Minneapolis, MN 55415, for defendant.

Defendant Mohamed Abdullah Warsame (“Warsame”) is charged with conspiracy to provide and providing material support and resources to a designated Foreign Terrorist Organization, in violation of 18 U.S.C. § 2339B, and with making false statements in violation of 18 U.S.C. § 1001(a)(2). Warsame has filed a motion for disclosure of applications for electronic surveillance under the Foreign Intelligence Surveillance Act of 1978 (“FISA”), and a motion to suppress evidence resulting from surveillance conducted pursuant to FISA. For the reasons discussed below, the Court denies these motions.

BACKGROUND

The Federal Bureau of Investigation (“FBI”) began investigating Warsame in July 2003 in connection with an international terrorism investigation. As part of that investigation, the FBI obtained orders from the United States Foreign Intelligence Surveillance Court authorizing electronic surveillance and searches of Warsame, including a wiretap of Warsame’s telephone and a physical search of his apartment. These orders were obtained pursuant to the certification procedures required under the Foreign Intelligence Surveillance Act, or FISA. 50 U.S.C. §§ 1801 *et seq.*

The FBI continued its surveillance activities until December 8, 2003, when agents approached Warsame for the first time at his home to discuss his background and travel experiences. Warsame agreed to accompany the agents to an undisclosed location, which turned out to be Camp Ripley, an Army National Guard military base in Little Falls, Minnesota. There, the questioning continued over the course of two days.¹ During these interviews, Warsame described some of his overseas experiences, including attending terrorist training camps in Afghanistan, receiving military training in an al Qaeda camp, and meeting Osama Bin Laden. Following these interviews, the agents drove Warsame back to the FBI office in Minneapolis, where he was arrested.

Warsame was subsequently charged with two counts of providing or conspiring to provide material support or resources to a foreign terrorist organization, and three counts

¹ On May 31, 2007, this Court issued an order granting in part Warsame’s motion to suppress evidence obtained during the interviews at Camp Ripley, finding that statements made during the final pre-arrest interview on December 9, 2003, were inadmissible because that interview amounted to custodial interrogation and Warsame was not given a Miranda warning. *United States v. Warsame*, 488 F. Supp. 2d 846, 860-61 (D. Minn. 2007).

of making false statements. The prosecution has notified Warsame that it intends to offer at trial evidence obtained and derived from the surveillance authorized by the Foreign Intelligence Surveillance Court. In response, Warsame filed a motion for disclosure of the FISA applications and related materials, arguing that disclosure of the FISA applications and orders is necessary for him to fully support his motion to suppress the evidence obtained from the surveillance and searches. Warsame has also filed a motion to suppress the fruits of the FISA surveillance, arguing that the surveillance applications fail to meet FISA's statutory certification requirements, and that FISA as amended by the Patriot Act violates the Fourth Amendment.

ANALYSIS

I. FOREIGN INTELLIGENCE SURVEILLANCE ACT

In 1978, Congress enacted the Foreign Intelligence Surveillance Act ("FISA"), which established detailed procedures governing the Executive Branch's ability to collect foreign intelligence information. FISA was a congressional response to the Supreme Court's decision in *United States v. United States District Court (Keith)*, 407 U.S. 297, 321-22 (1972), which expressly declined to decide whether the Fourth Amendment limits the President's power to conduct electronic surveillance to obtain foreign intelligence information for national security purposes. Through FISA, Congress sought to resolve "doubts about the constitutionality of warrantless, foreign security surveillance and yet protect the interests of the United States in obtaining vital intelligence about foreign powers." *ACLU Found. of S. Cal. v. Barr*, 952 F.2d 457, 461 (D.C. Cir. 1991).

FISA establishes a “secure framework” that seeks to balance the President’s power to conduct surveillance for foreign intelligence purposes with the individual rights guaranteed by the United States Constitution. *Id.* To obtain an order authorizing electronic surveillance or physical searches of an agent of a foreign power, FISA requires the government to file under seal an *ex parte* application with the United States Foreign Intelligence Surveillance Court (the “FISC”). 50 U.S.C. §§ 1804, 1823. The application must be approved by the Attorney General and must include certain specified information. *See* 50 U.S.C. §§ 1804(a), 1823(a). After review of the application, a single judge of the FISC enters an *ex parte* order granting the government’s application for electronic surveillance or a physical search of an agent of a foreign power, provided the judge makes certain specific findings.² 50 U.S.C. §§ 1805(a), 1824(a). 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. 50 U.S.C. §§ 1805(e)(2), 1824(d)(2).

As originally enacted, FISA also required the applications to contain a certification by a high-ranking Executive Official that “the purpose” of the surveillance was to obtain foreign intelligence information. 50 U.S.C. §§ 1804(a)(7)(B), 1823(a)(7)(B) (2000). In 2001, Congress enacted the Uniting and Strengthening America by Providing

² The FISA order must describe the target, the nature and location of the facilities or places to be searched, the information sought, and the means of acquiring such information. *See* 50 U.S.C. §§ 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 days or until the objective of the electronic surveillance or physical search has been achieved. *See* 50 U.S.C. §§ 1805(e)(1), 1824(d)(1).

Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (“Patriot Act”), which amended FISA to require only that “a significant purpose” of the surveillance or search is to obtain foreign intelligence information. 50 U.S.C. § 1804(a)(7)(B), 1823(a)(7)(B) (2006). By changing FISA’s purpose requirement, “Congress was keenly aware that this amendment relaxed a requirement that the government show that its primary purpose was other than criminal prosecution.” *In re Sealed Case*, 310 F.3d 717, 732 (Foreign Int. Surv. Ct. Rev. 2003).

In addition to imposing specific requirements on the Executive Branch, FISA allows the use of evidence derived from FISA surveillance and searches in criminal prosecutions. 50 U.S.C. §§ 1806(a), 1825(a). In this case, the prosecution has indicated that it intends to offer against Warsame certain evidence obtained and derived from electronic surveillance and physical searches authorized by the FISC. As required by FISA, the Attorney General has authorized the use of this FISA information in all phases of the prosecution of Warsame. *See* 50 U.S.C. §§ 1806(b), 1825(c). The prosecution has also provided defendant with the required written notice of its intent to use the FISA information. *See* 50 U.S.C. §§ 1806(c), 1825(d).

FISA also authorizes “an aggrieved person”³ to seek to suppress any evidence derived from FISA surveillance or searches on grounds that (1) the evidence was

³ FISA 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).

unlawfully acquired, or (2) the electronic surveillance or physical search was not conducted in conformity with the order of authorization or approval. 50 U.S.C. §§ 1806(e), 1825(f). Upon receiving notice of the prosecution's intent to use FISA information in his case, Warsame filed a motion for disclosure of the FISA applications and related materials. Warsame has also filed a motion to suppress information obtained pursuant to the FISC-authorized surveillance, arguing in part that the Patriot Act amendment to FISA violates his rights under the Fourth Amendment. For the reasons discussed below, the Court denies these motions.

II. MOTION TO DISCLOSE FISA MATERIALS

Warsame moves for the disclosure of all FISA applications, orders, and related documents as an "aggrieved person" under the Act. *See* 50 U.S.C. §§ 1806(e), 1825(f). Warsame asserts that disclosure of the FISA applications and orders is necessary for him to fully support his motion to suppress the evidence obtained from the surveillance and searches. Warsame contends that meaningful review cannot be accomplished through an *in camera*, *ex parte* review of the documents. Warsame further asserts that denial of disclosure would violate his right to due process.

In response to Warsame's request for disclosure, former Attorney General Alberto Gonzales filed an affidavit stating under oath that disclosure of such materials would harm national security. *See* 50 U.S.C. §§ 1806(f), 1825(g). In support of its claim of privilege, the United States submitted to the Court the sealed, classified declaration of John E. Lewis, Acting Assistant Director, Counterterrorism Division, Federal Bureau of

Investigation. Under FISA, the filing of an Attorney General affidavit triggers an *in camera, ex parte* procedure to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted. 50 U.S.C. §§ 1806(f), 1825(g). The Court's careful review of the sealed, classified materials fully supports the Attorney General's sworn assertion that the sealed materials filed with the Court contain

sensitive and classified information concerning United States intelligence sources and methods and other information relating to efforts of the United States to conduct counterintelligence investigations, including the manner and means by which those investigations are carried out; [and that] to reveal such information reasonably could be expected to cause serious and exceptionally grave damage to the national security of the United States.

(Declaration and Claim of Privilege of the Attorney General of the United States, at 3.)

Once the *in camera, ex parte* procedure is triggered, the reviewing court may disclose such materials "only where such disclosure is necessary to make an accurate determination of the legality of the surveillance." 50 U.S.C. § 1806(f); *see also* 50 U.S.C. § 1825(g). The legislative history explains that such disclosure is "necessary" only where the court's initial review indicates that the question of legality may be complicated by factors such as

indications of possible misrepresentation of fact, vague identification of the persons to be surveilled, or surveillance records which include a significant amount of nonforeign intelligence information, calling into question compliance with the minimization standards contained in the order.

United States v. Belfield, 692 F.2d 141, 147 (D.C. Cir. 1982) (quoting S. Rep. No. 95-701, 95th Cong., 2d Sess. 64 (1978)).

No United States District Court or Court of Appeals has ever determined that disclosure to the defense of such materials was necessary to determine the lawfulness of

surveillance or searches under FISA. *See United States v. Rosen*, 447 F. Supp. 2d 538, 546 (D. Va. 2006) (collecting cases). Warsame attempts to distinguish these cases by pointing to recent government admissions that numerous FISA applications have included misstatements and critical omissions. *See In re All Matters Submitted to the Foreign Intelligence Surveillance Court*, 218 F. Supp. 2d 611, 620-21 (Foreign Int. Surv. Ct. 2002) (discussing errors discovered in more than 75 FISA applications). Warsame further argues that the consistency of these case holdings demonstrates that the FISA process is a “sham,” and that adversarial proceedings are particularly important here because of the complexity of the issues presented to the Court.

The Court is receptive to Warsame’s concerns about the one-sided nature of the FISA process, and has engaged in a comprehensive and careful review of the FISA applications, orders, and other related materials. However, the Court has found that the issues presented by the FISA applications are straightforward and uncontroversial, and present none of the concerns that might warrant disclosure. The fact that the government has included misstatements and critical omissions in other FISA applications not at issue here cannot justify disclosure in this case. Without some indication that the congressionally mandated FISA procedures were not followed here, the government’s legitimate national security interest in maintaining the secrecy of the information contained in the FISA applications bars disclosure of the materials to Warsame.

The Court further concludes that the *ex parte* procedure complies with due process.⁴ Warsame argues that *Mathews v. Eldridge*, 424 U.S. 319 (1976), provides the appropriate analytical framework for determining whether due process requires disclosure. *Mathews* held that courts should consider three factors when determining whether a practice violates the right to procedural due process:

First, the private interest that will be affected by the official action; second, the risk of an erroneous deprivation of such interest through the procedures used, and the probable value, if any, of additional or substitute procedural safeguards; and finally, the Government's interest, including the function involved and the fiscal and administrative burdens that the additional or substitute procedural requirement would entail.

Id. at 335. The prosecution disputes that the *Mathews* framework is appropriate for assessing the validity of FISA procedures in the context of criminal cases, noting that no federal court that has examined the constitutionality of FISA's *in camera*, *ex parte* procedure has even considered *Mathews*. Indeed, the Supreme Court has held that the *Mathews* balancing test is generally inappropriate in criminal cases. *See Medina v. California*, 505 U.S. 437, 444-45 (1992). As the *Medina* Court explained, the Bill of Rights itself is the source of constitutional guarantees required in criminal proceedings. *Id.* at 443. "[T]he expansion of those constitutional guarantees under the open-ended rubric of the Due Process Clause invites undue interference with both considered legislative judgments and the careful balance that the Constitution strikes between liberty and order." *Id.*; *see also Krimstock v. Kelly*, 464 F.3d 246, 254 (2d Cir. 2006) (noting

⁴ Warsame also asserts that denial of disclosure would deny him his right to effective assistance of counsel. The Court finds this assertion to be without merit. *See, e.g., United States v. Nicholson*, 955 F. Supp. 588, 592 (E.D. Va. 1997). Because Warsame does not provide any supporting argument for this assertion, the Court will not further address the issue.

that the *Mathews* framework is inappropriate for resolving challenges to the process afforded in criminal proceedings). The Court is therefore not convinced that the *Mathews* balancing test supplies an appropriate framework for evaluating FISA procedures in this case.

Even applying the *Mathews* framework, however, the Court finds that due process does not mandate disclosure of the FISA materials to Warsame. There is no doubt that Warsame has important privacy and liberty interests at stake, and the Court recognizes the difficulty faced by defense counsel in this situation. The defense must argue for the suppression of information gained from FISA surveillance without ever seeing the basis for the court orders authorizing the surveillance. Nevertheless, the Court does not think that disclosure of the FISA materials to Warsame is the appropriate response to this concern. FISA attempts to protect the rights of individuals not through mandatory disclosure but through “in-depth oversight of FISA surveillance by all three branches of government and by a statutory scheme that to a large degree centers on an expanded conception of minimization that differs from that which governs law-enforcement surveillance.” *Belfield*, 692 F.2d at 148. Given these protections, and based on the Court’s careful review of the FISA materials in this case, the Court believes that the probable value of disclosure, as well as the risk of nondisclosure, of the FISA materials to the defense is low. Finally, the government has a substantial national security interest in

preventing the disclosure of these materials, which was persuasively articulated in a sealed affidavit of the Attorney General.⁵

In sum, the Court concludes that disclosure of FISA materials to Warsame is not necessary for an accurate determination of the legality of the surveillance, and not necessary to adequately safeguard Warsame's due process rights. Warsame's motion for disclosure is therefore denied.

III. MOTION TO SUPPRESS FOR FAILURE TO SATISFY FISA'S STATUTORY REQUIREMENTS

Warsame next argues that evidence resulting from FISA surveillance and searches in this case should be suppressed because the government's FISA applications failed to satisfy FISA's statutory requirements. Under § 1806(f), if an aggrieved person moves to suppress FISA evidence, the Court must review *ex parte* and *in camera* the government's applications, as well as the Foreign Intelligence Surveillance Court orders authorizing the surveillance, to determine whether the surveillance was lawfully authorized and conducted. In making this determination, the Court must find that:

- (1) the President has authorized the Attorney General to approve applications for electronic surveillance for foreign intelligence information;

⁵ Warsame asserts that the national security interest can be adequately protected even if the FISA materials are disclosed to the defense because his defense attorney has the high-level security clearance necessary to view the materials. The Court finds this argument unpersuasive. In FISA, Congress reasonably authorized the Attorney General to invoke an *ex parte* procedure to ensure that sensitive security information is not unnecessarily disseminated to anyone not involved in the surveillance operation in question. *United States v. Ott*, 827 F.2d 473, 477 (9th Cir. 1987).

- (2) the application has been made by a Federal officer and approved by the Attorney General;
- (3) on the basis of the facts submitted by the applicant there is probable cause to believe that—
 - (A) the target of the electronic surveillance is a foreign power or an agent of a foreign power: *Provided*, That no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States; and
 - (B) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power;
- (4) the proposed minimization procedures meet the definition of minimization procedures under section 1801 (h) of this title; and
- (5) the application which has been filed contains all statements and certifications required by section 1804 of this title 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 section 1804(a)(7)(E) of this title and any other information furnished under section 1804(d) of this title.

50 U.S.C. § 1805(a).⁶

The Court has carefully reviewed the relevant FISA certifications, minimization procedures, and probable cause determinations, pursuant to 50 U.S.C. § 1805(a) and as set forth below. Because the FISA review is *ex parte*, the Court rejects the prosecution’s contention that the FISC’s probable cause determinations are entitled to “substantial deference.” *See Rosen*, 447 F. Supp. 2d at 545 (stating that review is *de novo*, “especially

⁶ Similar requirements apply in the case of physical searches under 18 U.S.C. § 1824(a), and the Court’s suppression analysis is identical for electronic surveillance and physical searches.

given that the review is *ex parte* and thus unaided by the adversarial process.”); *United States v. Squillacote*, 221 F.3d 542, 554 (4th Cir. 2000) (same). As such, the FISA materials 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* 50 U.S.C. § 1805(a)(5) (applying “clearly erroneous” standard to factual averments contained in certifications when the target is a United States person); *Rosen*, 447 F. Supp. 2d at 545.

A. Certifications

A careful review of the relevant FISA materials in this case reveals that the applications and the resulting FISC orders satisfy the statutory requirements under 50 U.S.C. § 1805(a). The President authorized the Attorney General to approve the applications to the FISC, and each of the applications was made by a federal officer and approved by the Attorney General or his authorized designate. *See* 50 U.S.C. § 1805(a)(1), (2). The Court further finds that the applications contain all required statements and certifications, and that the certifications are not clearly erroneous based on statements made under § 1804(a)(7)(E).⁷ *See* 50 U.S.C. § 1805(a)(5).

B. Minimization Procedures

The proposed minimization procedures contained in the applications and FISA orders also must meet the statutory requirements of 50 U.S.C. § 1801(h). *See* 50 U.S.C.

⁷ Under § 1804(a)(7)(E), the certification must include a statement that the information sought is the type of foreign intelligence information designated, and that such information cannot reasonably be obtained by normal investigative techniques.

§ 1805(a)(4). 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 at 731. However, in enacting FISA, “Congress recognized that ‘no electronic surveillance can be so conducted that innocent conversations can be totally eliminated.’” *United States v. Hammoud*, 381 F.3d 316, 334 (4th Cir. 2004) (quoting S. Rep. No. 95-701, at 39 (1978)), *vacated on other grounds*, 543 U.S. 1097 (2005).

The minimization procedures require the government to make a good faith effort to minimize the acquisition and retention of irrelevant information. *Id.* Based on a careful and searching review of the FISA warrant applications and orders in this case, the Court finds that the proposed minimization procedures contained in these materials satisfy the statutory requirements of § 1801(h).

C. Probable Cause

Before authorizing surveillance, a FISA judge must also determine that there is probable cause to believe that “the target of the electronic surveillance is . . . 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 . . . an agent of a foreign power.” 50 U.S.C. § 1805(a)(3).⁸ A “foreign power” includes “a group engaged in international terrorism or activities in preparation therefor.” § 1801(a)(4). As it relates to

⁸ Similar requirements apply in the context of physical searches, 50 U.S.C. § 1824(a)(3), and this analysis applies both to electronic surveillance and physical searches.

United States citizens or aliens lawfully admitted for permanent residence, “agent of a foreign power” includes:

[A]ny person who –

...

(C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power; [or]

...

(E) knowingly aids or abets any person in the conduct of activities described in subparagraph . . . (C) or knowingly conspires with any person to engage in activities described in subparagraph . . . (C).

50 U.S.C. § 1801(b)(2).

Probable cause is a “fluid concept – turning on the assessment of probabilities in particular factual contexts – not readily, or even usefully, reduced to a neat set of legal rules.” *Illinois v. Gates*, 462 U.S. 213, 232 (1983). In evaluating whether probable cause exists in a given case, the issuing judge must “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.* at 238; *United States v. Grant*, 490 F.3d 627, 631-32 (8th Cir. 2007).⁹ Further, in making probable cause determinations under

⁹ Under FISA, a reviewing judge may not make a probable cause determination “solely upon the basis of activities protected by the first amendment to the Constitution of the United States.” 50 U.S.C. § 1805(a)(3)(A). However, 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.” *Rosen*, 447 F. Supp. 2d at 548; *see United States v. Dumeisi*, 424 F.3d 566, 579 (7th Cir. 2005). Based on a review of the FISA applications, the Court is satisfied that Warsame’s First Amendment rights have not been violated in this case.

FISA, a reviewing judge may “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).

The Court has carefully reviewed the materials submitted to the FISC in support of the FISA applications in this case. Based on a review of those materials, the Court finds that probable cause existed to believe that Warsame was an agent of a foreign power, namely, al Qaeda, in accordance with FISA’s statutory requirements. The Court further finds there was probable cause to believe that each of the places to be searched, and the places where surveillance was to be conducted, was being used, or was about to be used, by Warsame.

In sum, the Court concludes that the FISA applications, including the relevant certifications, minimization procedures, and probable cause determinations, are in compliance with the statutory requirements under §§ 1805(a) and 1824(a). Accordingly, the Court denies Warsame’s motion to suppress to the extent it is based on a violation of FISA’s statutory requirements.

IV. MOTION TO SUPPRESS BASED ON FOURTH AMENDMENT VIOLATIONS

Warsame argues that FISA search and surveillance orders violate the Fourth Amendment because FISA does not require a sufficient showing of probable cause or particularity. Warsame further argues that FISA’s “significant purpose” requirement, as amended by the Patriot Act, violates his rights under the Fourth Amendment. The Court addresses each argument in turn.

A. The Fourth Amendment Requirements of Probable Cause and Particularity

As discussed above, FISA requires a showing of probable cause to believe that the target of the electronic surveillance or search is a foreign power or an agent of a foreign power. 50 U.S.C. §§ 1805(a)(3)(A), 1824(a)(3)(A). FISA also requires probable cause to believe that each of the facilities or places at which 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 or property to be searched is owned, used, or possessed by a foreign power or an agent of a foreign power. 50 U.S.C. §§ 1805(a)(3)(B), 1824(a)(3)(B). Warsame argues that FISA's probable cause requirements do not satisfy the Fourth Amendment because they do not require a showing that the foreign power or its agent has, is, or is about to commit a terrorist activity or crime, or that the facilities or places to be searched will contain or produce evidence of terrorist or criminal activity. Warsame further argues that FISA does not require any showing of particularity with respect to the area to be searched or the items to be seized.¹⁰

In *United States v. United States District Court (Keith)*, 407 U.S. 297, 299 (1972), the Supreme Court addressed the “delicate question of the President’s power, acting

¹⁰ Warsame also argues that a FISA order is not a “warrant” within the meaning of the Fourth Amendment. However, courts upholding the constitutionality of FISA have done so not because a FISA order is a “warrant,” but because the need for foreign intelligence justifies an exception to the warrant requirement, and because FISA strikes a reasonable balance between governmental interests in national security and individual liberty interests. See *In re Sealed Case*, 310 F.3d at 726 (explaining that courts of appeals have upheld FISA based on the President’s authority to conduct warrantless surveillance where the “primary purpose” of the surveillance is foreign intelligence gathering); see also *United States v. United States Dist. Court*, 407 U.S. 297, 322-23 (1972) (stating that the warrant requirement “may vary according to the governmental interest to be enforced and the nature of citizen rights deserving protection”).

through the Attorney General, to authorize electronic surveillance in internal security matters without prior judicial approval.” The Court held that such judicial approval is necessary to satisfy the Fourth Amendment in conducting domestic security surveillance, but it specifically declined to address the scope of the President’s surveillance power with respect to foreign intelligence. *Id.* at 323-24. However, *Keith* took care to explain that the specific statutory requirements for electronic surveillance of “ordinary crime” under Title III¹¹ – including the requirement of probable cause to believe an individual has, is, or is about to commit a crime – were not constitutionally mandated in the context of domestic security surveillance for national security purposes. *Id.* at 322. Noting that domestic security surveillance involves different policy and practical considerations from surveillance of “ordinary crime,” *Keith* stated that “the focus of domestic surveillance may be less precise than that directed against more conventional types of crime.” *Id.* Thus, the appropriate Fourth Amendment inquiry is one of reasonableness: “Different standards may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens.” *Id.* at 322-23.

The Supreme Court’s decision in *Keith* makes clear that the probable cause required by the Fourth Amendment is not necessarily probable cause to believe that a

¹¹ Title III of the Omnibus Crime Control and Safe Streets Act of 1968 authorizes electronic surveillance for certain classes of domestic crimes. 18 U.S.C. §§ 2510 *et seq.* Title III requires, among other things, probable cause to believe that an individual is committing, has committed, or is about to commit a specified predicate offense, § 2518(3)(a); probable cause to believe that particular communications concerning the specified crime will be obtained through interception, § 2518(3)(b); that the information sought is not available through normal investigative procedures, § 2518(3)(c); and that the orders authorizing electronic surveillance may last only up to 30 days. § 2518(5).

crime was committed, is being committed, or is about to be committed. *See id.*; *see also United States v. Ning Wen*, 477 F.3d 896, 898 (7th Cir. 2007) (“[T]he probable cause of which the fourth amendment speaks is not necessarily probable cause to believe that any law is being violated.”). Rather, the appropriate inquiry here is whether the probable cause and particularity that FISA *does* require satisfy the Fourth Amendment’s reasonableness requirement. *United States v. Cavanagh*, 807 F.2d 787, 790 (9th Cir. 1987); *United States v. Duggan*, 743 F.2d 59, 72 (2d Cir. 1984) (stating that the implication of *Keith* is that “the warrant requirement is flexible and that different standards may be compatible with the Fourth Amendment in light of the different purposes and practical considerations of domestic national security surveillances”). The question whether FISA violates the Fourth Amendment is an issue of first impression in this circuit. The Court notes, however, that prior to the amendment of FISA in 2001, every court to have considered this issue has upheld FISA on constitutional grounds. *See, e.g., United States v. Johnson*, 952 F.2d 565, 573 (1st Cir. 1991); *United States v. Pelton*, 835 F.2d 1067, 1075 (4th Cir. 1987); *Duggan*, 743 F.2d at 73; *Global Relief Found., Inc. v. O’Neill*, 207 F. Supp. 2d 779, 807 (N.D. Ill. 2002).

The Court agrees with the unanimous holdings of these courts and finds that, where the primary purpose of the government’s surveillance is foreign intelligence gathering, FISA’s probable cause and particularity requirements satisfy the reasonableness requirement of the Fourth Amendment.¹² As to the government’s interest,

¹² The Court addresses the implications of the “significant purpose” amendment on FISA’s constitutionality below. Because the government surveillance in this case was primarily

there can be little question that foreign intelligence gathering is of the utmost importance in protecting the national security interests of the United States. *See, e.g., Pelton*, 835 F.2d at 1075 (stating that the governmental interest in gathering foreign intelligence is of “paramount importance” to national security interests). Similar to the domestic security surveillance discussed in *Keith*, foreign intelligence gathering involves different policy considerations from the surveillance of ordinary criminal activity. FISA’s probable cause and particularity requirements reflect the inherent difficulties in detecting national security threats and the government’s increased emphasis on prevention and preparedness in the national security context. *Cf. Keith*, 407 U.S. at 322 (discussing similar considerations in the context of domestic security surveillance).

At the same time, FISA provides safeguards that are designed to protect individual rights guaranteed by the Fourth Amendment. The Fourth Amendment protects individuals against “unreasonable searches and seizures,” including unreasonable surveillance that intrudes upon individual privacy and free expression, and requires that warrants be supported by probable cause and particularly describe the places to be searched and the persons or things to be seized. U.S. Const. amend. IV; *Keith*, 407 U.S. at 315-16. FISA requires probable cause to believe that the target is acting “for or on behalf of a foreign power,” 50 U.S.C. § 1801(b)(2), and thus applies “only to certain carefully delineated, and particularly serious, foreign threats to national security.” *In re Sealed Case*, 310 F.3d at 739; *Duggan*, 743 F.2d at 73. As to particularity, FISA requires

directed at foreign intelligence, however, Warsame’s motion requires the Court to consider the constitutionality of FISA in cases where the government certifies that its primary purpose is foreign intelligence gathering.

probable cause to believe that each of the facilities or places at which the surveillance is directed is being used, or is about to be used, by a foreign power or its agent. *See* 50 U.S.C. §§ 1805(a)(3)(B), 1824(a)(3)(B); *In re Sealed Case*, 310 F.3d at 740 (“[F]ISA 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.”). Like Title III, FISA requires a finding that the information sought cannot reasonably be obtained through normal investigative techniques. *Compare* 50 U.S.C. § 1804(a)(7)(E)(ii), *with* 18 U.S.C. § 2518(3)(c). And while FISA orders may last up to 90 days,¹³ instead of the 30-day limit of Title III, this difference reflects the reality that national security surveillance is “often long range and involves the interrelation of various sources and types of information.” *Keith*, 407 U.S. at 322; *In re Sealed Case*, 310 F.3d at 740.

In sum, the Court finds that, where the primary purpose of the government’s surveillance is foreign intelligence gathering, FISA’s requirements strike a reasonable balance between the government’s interest in national security and individual privacy interests under the Fourth Amendment. The Court therefore concludes that FISA complies with the probable cause and particularity requirements of the Fourth Amendment, and denies Warsame’s motion to suppress on this basis.

¹³ FISA orders may be valid for up to 90 days for a “United States person,” as that term is defined in 50 U.S.C. § 1801(i), or up to 120 days for a non-“United States person.” 50 U.S.C. §§ 1805(e), 1824(d).

B. FISA’s “Significant Purpose” Requirement

Warsame also argues that FISA’s “significant purpose” requirement, as amended by the Patriot Act, violates the Fourth Amendment. Prior to the enactment of the Patriot Act, FISA required executive branch officials to certify to a FISA judge “that the purpose of the surveillance is to obtain foreign intelligence information.” 50 U.S.C. § 1804(a)(7)(B) (2000). Courts interpreted FISA’s “the purpose” language to require a showing that “the primary purpose” of the surveillance is to obtain foreign intelligence. *See, e.g., Duggan*, 743 F.2d at 77; *Johnson*, 952 F.2d at 572.

The “primary purpose” standard was consistent with pre-FISA decisions holding that warrantless surveillance by the executive branch was permissible *only* if the purpose of the surveillance was primarily to gather foreign intelligence information. *See, e.g., United States v. Butenko*, 494 F.2d 593, 601 (3d Cir. 1974) (noting that the surveillance was conducted “solely for the purpose of gathering foreign intelligence information”); *United States v. Truong Dinh Hung*, 629 F.2d 908, 915 (4th Cir. 1980) (finding that the executive branch is excused from the warrant requirement only when “the object of the search or the surveillance is a foreign power,” and “the surveillance is conducted ‘primarily’ for foreign intelligence reasons”). The “primary purpose” requirement ensured that law enforcement officials availed themselves of FISA’s more flexible certification procedures only if they primarily sought to obtain foreign intelligence information. In other words, courts imposed the “primary purpose” standard to ensure that law enforcement could not make an “end-run” around the stricter requirements of Title III and the Fourth Amendment in the context of ordinary criminal prosecution. *See*

Johnson, 952 F.2d at 572. By requiring law enforcement to show that the “primary purpose” of the surveillance was to obtain foreign intelligence information, courts were assured that the primary purpose was *not* the prosecution of ordinary crime. As discussed above, prior to the Patriot Act amendment, courts uniformly held that FISA procedures were consistent with the Fourth Amendment.

When Congress enacted the Patriot Act in October 2001, however, it amended FISA to allow electronic surveillance and searches where “a significant purpose” of the surveillance or search was to obtain foreign intelligence information. 50 U.S.C. §§ 1804(a)(7)(B), 1823(a)(7)(B). The amendment was intended to break down the traditional barriers – commonly referred to as the “wall” – that had existed between criminal law enforcement and intelligence gathering. *In re Sealed Case*, 310 F.3d at 732-33 (citing 147 Cong. Rec. S10992 (Oct. 25, 2001) (statement of Sen. Leahy)). By allowing a FISA order to issue where “a significant purpose” is foreign intelligence gathering, FISA now allows surveillance and searches even where the primary purpose of the surveillance is criminal prosecution, so long as “a significant purpose” of the surveillance or search is to obtain foreign intelligence. *Id.*

Since the Patriot Act amendment, all but one court have upheld FISA as consistent with the requirements of the Fourth Amendment. *See, e.g., United States v. Damrah*, 412 F.3d 618, 625 (6th Cir. 2005); *United States v. Benkahla*, 437 F. Supp. 2d 541 (E.D. Va. 2006). In *In re Sealed Case*, for example, the Foreign Intelligence Surveillance Court of Review upheld the constitutionality of the “significant purpose” requirement, and rejected the pre-Patriot Act interpretation of FISA as requiring a “primary purpose” of

foreign intelligence gathering, noting that much of FISA's statutory language was itself "grounded on criminal conduct."¹⁴ *In re Sealed Case*, 310 F.3d at 723 (tracing the history and development of the "primary purpose" standard). The court construed the "significant purpose" requirement as permitting surveillance even where the government's primary purpose is criminal prosecution for foreign intelligence crimes, although it would not allow "a primary objective of prosecuting an agent for a non-foreign intelligence crime," and would not allow surveillance where "a sole objective" is criminal prosecution. *Id.* at 735-36. Comparing FISA to the requirements of Title III, the court ultimately found that FISA and the "significant purpose" requirement struck a reasonable balance between governmental interests in national security and individual privacy interests. *Id.* at 744-45.

As these cases make clear, however, the "significant purpose" requirement implicates significant Fourth Amendment concerns to the extent that it now permits FISA surveillance where the primary purpose of the surveillance is criminal prosecution. The Foreign Intelligence Surveillance Court of Review itself acknowledged that the question "whether Congress' disapproval of the primary purpose test is consistent with the Fourth Amendment . . . has no definitive jurisprudential answer." *Id.* at 746. The legislative history of the Patriot Act amendment demonstrates that members of Congress had serious doubts about the constitutionality of the "significant purpose" requirement. *Id.* (noting that the Chairman of the Senate Judiciary Committee found the amendment "very

¹⁴ The court focused in particular on FISA's definition of "agent" and "international terrorism," noting that these words are defined largely in terms of criminal activity. *In re Sealed Case*, 310 F.3d at 723.

problematic” because it allows FISA surveillance “where the Government’s most important motivation for the wiretap is for use in a criminal prosecution”) (quoting 147 Cong. Rec. S10593 (Oct. 11, 2001)). At least one district court has since determined that the “significant purpose” test violates the Fourth Amendment. *See Mayfield v. United States*, 504 F. Supp. 2d 1023, 1038 (D. Or. 2007) (striking down Patriot Act amendment because “the primary purpose of the electronic surveillance and physical searching of [plaintiff]’s home was to gather evidence to prosecute him for crimes”). Indeed, to the extent FISA now allows warrantless surveillance where the government’s primary purpose is criminal prosecution, the “significant purpose” standard is in tension with settled precedent upholding FISA on grounds that the President has inherent authority to conduct warrantless surveillance *only* if it is intended primarily for foreign intelligence gathering.

Despite these concerns, however, FISA’s “significant purpose” requirement necessarily encompasses situations in which the government certifies that its primary purpose is foreign intelligence gathering, and not criminal prosecution. As discussed above, courts have unanimously concluded that the Fourth Amendment is satisfied where law enforcement certifies that its primary purpose in conducting FISA surveillance is to gather foreign intelligence. Thus, at least as it applies to situations in which the primary purpose of the government’s FISA surveillance remains foreign intelligence gathering, the Court finds that the “significant purpose” requirement is within the limits of the Fourth Amendment. *See Hammoud*, 381 F.3d at 333-34 (finding post-Patriot Act FISA surveillance permissible where law enforcement was primarily interested in obtaining

foreign intelligence information); *United States v. Mubayyid*, 2007 WL 3287393, at *11 (D. Mass. Nov. 5, 2007) (same).

The Court shares the very significant concerns that the “significant purpose” standard violates the Fourth Amendment. Ultimately, however, the Court need not decide the issue here. Based on a careful review of the FISA applications and orders in this case, the Court is satisfied that the primary purpose of the FISA surveillance and searches was to gather foreign intelligence, and was not to prosecute Warsame for criminal activity. As such, the Court concludes that FISA’s “significant purpose” requirement is not unconstitutional as it applies to the FISA orders in this case. Warsame’s motion to suppress based on the unconstitutionality of FISA is therefore denied.

CONCLUSION

The Court has significant concerns over the delays inherent in a case, such as this one, which requires extensive application of the Classified Information Procedures Act. The delays are complicated further by the still-pending appeal to the Eighth Circuit Court of Appeals taken by the government. Once the Eighth Circuit issues its opinion and the opinion becomes final, the Court anticipates setting a firm trial date as soon as possible. Counsel should be prepared for trial.

ORDER

Based on the foregoing, all the records, files, and proceedings herein, **IT IS HEREBY ORDERED** that:

1. Warsame's Motion for Disclosure of FISA Applications, Orders, and Related Documents [Docket No. 38] is **DENIED**.

2. Warsame's Motion to Suppress the Fruits of All Surveillance and Each Search Conducted Under FISA [Docket No. 43] is **DENIED**.

DATED: April 17, 2008
at Minneapolis, Minnesota.

s/ John R. Tunheim
JOHN R. TUNHEIM
United States District Judge