

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO

CASE NO. 12-cr-00033-JLK

UNITED STATES OF AMERICA,

Plaintiff,

v.

1. **JAMSHID MUHTOROV,**

Defendant.

**MOTION TO SUPPRESS FISA ACQUIRED
EVIDENCE (SUPPLEMENT TO DOC. 14)**

Mr. Muhtorov, through counsel, Brian R. Leedy, Assistant Federal Public Defender, and pursuant to 50 U.S.C. §§ 1806(e) and 1825(f), respectfully requests the suppression of any evidence obtained or derived from electronic surveillance or physical searches conducted pursuant to the Foreign Intelligence Surveillance Act (FISA) (50 U.S.C. §§ 1801-1811, 1821-1829), sought to be offered into evidence, or otherwise used or disclosed by the government. As grounds he states as follows:

On February 7, 2012, the government filed a “Notice of Intent to Use Foreign Intelligence Surveillance Information,” stating their intent to “offer into evidence or otherwise use or disclose in any proceedings in the above captioned matter information obtained and derived from electronic surveillance and physical search conducted pursuant to” FISA. The government’s notice was provided pursuant to 50 U.S.C. §§ 1806(c) and 1825(d), which refer to the notification requirements for the use of FISA

information acquired from electronic surveillance and physical searches, respectively.

Doc. 12.

50 U.S.C. §§ 1806(e) and 1825(f) provide that “[a]ny person against whom evidence obtained or derived from” FISA acquired electronic surveillance or physical search “to which he is an aggrieved person¹ is to be, or has been, introduced or otherwise used or disclosed in any trial, hearing, or other proceeding in or before any court . . . may move to suppress the evidence obtained or derived from such search on the grounds that the information was unlawfully acquired; or the physical search was not made in conformity with an order of authorization or approval.”²

All evidence obtained and derived from FISA surveillance or searches should be suppressed because the FISA applications may fail to establish probable cause that Mr. Muhtorov is an “agent of a foreign power,” the applications may contain intentional or

¹ An “[a]ggrieved person” is “a person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance.” 50 U.S.C. § 1801(k)

² 50 U.S.C. §§ 1806(f) and 1825(g) provide that whenever a court is notified of the government’s intent to enter into evidence, or otherwise use, information obtained through electronic surveillance or physical searches made pursuant to FISA, or whenever any motion to suppress such evidence is made pursuant to 50 U.S.C. §§ 1806(e), or 1825(f), the “United States district court . . . shall, notwithstanding any other provision of law, if the Attorney General files an affidavit under oath that disclosure or any adversary hearing would harm the national security of the United States, review in camera and ex parte the application, order, and such other materials relating to the physical search as may be necessary to determine whether the physical search of the aggrieved person was lawfully authorized and conducted.” 50 U.S.C. §§ 1806(f) and 1825(g) further provide that “[i]n making this determination, the court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the physical search, or may require the Attorney General to provide to the aggrieved person a summary of such materials, only where such disclosure is necessary to make an accurate determination of the legality of the physical search.”

reckless material falsehoods or omissions, minimizations procedures may be inadequate, and the government may have failed to comply with minimization procedures, the government may not have made the required certifications in FISA applications, or those certifications may have been erroneous, and any extensions of FISA applications based on searches performed are fruit of the poisonous tree and should be suppressed.³

I. INTRODUCTION

This case involves numerous intrusive searches of Mr. Muhtorov's private residence, his computer, email accounts, and personal effects. According to the Affidavit attached to the Complaint (Document No. 1), The Federal Bureau of Investigation (FBI) began investigating Mr. Muhtorov based on “communications with www.soldiglar.com website administrator and Islamic Jihad Union (“IJU”) facilitator” known as “Abu Muhammad”. Doc. 1, pg. 4. The Affidavit states that “[p]ursuant to court authorization,” the FBI obtained communications via email regularly accessed through a laptop computer, and communications originating from Mr. Muhtorov’s phone lines. *Id.*

The searches at issue violate the Fourth Amendment to the United States Constitution, which protects “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.” U.S. CONST. AM. IV. The searches appear to have been conducted pursuant to an

³ Mr. Muhtorov has not had access to the underlying FISA materials, and as such, can only speculate as to their inadequacies. If the Court grants Mr. Muhtorov’s motion for access to FISA materials, he will seek leave to supplement this motion.

authorization under the Foreign Intelligence Surveillance Act (FISA), which, as shown herein, was designed for foreign intelligence gathering but is increasingly used by law enforcement to circumvent the protections of the Fourth Amendment and other vital Constitutional protections.

This supplement will explain first, as far as can be determined without access to the FISA materials, that the protocol for obtaining a FISA order was not followed in this case and, consequently, that the fruits of the FISA search should be suppressed. Second, the numerous reasons why the defense should be given access to the FISA materials in this case. And finally, why this Court should rule that FISA is unconstitutional on its face and as applied in this case.

II. FISA OVERVIEW

FISA, enacted in 1978, established the Foreign Intelligence Surveillance Court (FISC), a unique type of court that operates in secret and in which the government is the only entity permitted to appear. FISA authorizes issuance of two types of warrants that may be issued by the FISC – those allowing electronic surveillance and those allowing physical searches. Both types of warrants are at issue in this case, as the Complaint establishes that electronic and physical searches occurred prior to the issuance of a warrant and pursuant to "legally authorized surveillance" (i.e., FISA). Complaint Affidavit (Doc. No. 3) at 17 (electronic surveillance), 31 (physical searches).

The statutory prerequisites of FISA are the same in most respects for both electronic and physical intrusions. Any application to the FISC must be made under oath by a federal officer and contain certain information and certifications. 50 U.S.C.

§§ 1804 and 1823. In brief, an application for electronic surveillance or a physical search must:

- provide the identity of the Federal officer making the application;
- state the identity or description of the target;
- include a statement of the facts and circumstances relied upon by the applicant to justify his belief that the target of the search or surveillance is a foreign power or an agent of a foreign power and 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;
- provide a "statement of proposed minimization procedures";
- provide a description of the nature of the information sought and the type of communications or activities to be subjected to surveillance;
- set forth "certifications" by the Assistant to the President for National Security Affairs, an executive branch official or officials designated by the President from among those executive officers employed in the area of national security or defense and appointed by the President with the advice and consent of the Senate, stating as follows:
 - (A) the certifying official deems the information sought to be foreign intelligence information;
 - (B) a significant purpose of the search or surveillance is to obtain foreign intelligence information;
 - (C) such information cannot reasonably be obtained by normal investigative techniques,
 - (D) the type of foreign intelligence information being sought according to the categories describe in section 1801(e); and
 - (E) the basis for the certification that -
 - (i) the information sought is the type of foreign intelligence information designated; and

- (ii) such information cannot reasonably be obtained by normal investigative techniques.

50 U.S.C. §§ 1804(a), 1823(a).

The statute also requires a summary statement of the means by which the surveillance will be effected and a statement whether physical entry is required to effect the surveillance, including:

- a statement of facts concerning all previous applications that have been made to any judge under this statute and action taken on each previous application;
- the specific period of time for which the electronic surveillance is required to be maintained.

Id. § 1804(a)(7) - (9).

The Attorney General must personally review the application and determine that it satisfies the criteria and requirements set forth in the statute. *Id.* at § 1804(d).

A. Requirements to Obtain a FISA Order and Standard for Suppression of FISA Evidence.

At the outset it will be helpful to emphasize some of FISA's more important requirements. Before the FISA court can approve electronic surveillance or a physical search, it must make several important findings. One of the more important aspects of a FISA order is that the government must show facts that "the target of the electronic surveillance is a foreign power or an agent of a foreign power" and that each of the facilities or places at which the electronic surveillance or physical search is directed is being used, or is about to be used, by the foreign power or an agent thereof.

50 U.S.C. §§ 1804(a)(3); 1824(a)(2).

Additionally, FISA requires a "certification or certifications by the Assistant to the President for National Security Affairs, an executive branch official or officials designated by the President from among those executive officers employed in the area of national security or defense and appointed by the President with the advice and consent of the Senate, or the Deputy Director of the Federal Bureau of Investigation, if designated by the President as a certifying official," that a significant purpose of the surveillance or search is to obtain foreign intelligence information." 50 U.S.C. §§ 1804(a)(6)(B), 1823(a)(6)(B).

Also importantly, FISA authorizes any "aggrieved person" to move to suppress evidence obtained or derived from electronic surveillance or a physical search on the grounds that the information was unlawfully acquired, or the surveillance or search was not made in conformity with an order of authorization or approval. *Id.* at §§ 1806(e), 1825(f). FISA defines the phrase "aggrieved person" as "a person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance." *Id.* at § 1801(k).

B. This Court's Standard of Review of the FISA Application and Procedure is De Novo.

This Court should review the FISA applications and orders de novo. *United States v. Hammound*, 381 F.3d 316, 332 (4th Cir. 2004) (noting district court's de novo review and conducting its own de novo review of FISA materials), vacated on other grounds, 543 U.S. 1097 (2005); *United States v. Squillacote*, 221 F.3d 542, 554 (4th Cir. 2000) (same). Indeed, a reviewing court should conduct essentially the same review of the FISA application and materials that the FISC conducted. *In re Grand Jury*

Proceedings of the Special April 2002 Grand Jury, 347 F.3d 197, 204-05 (7th Cir. 2003). And "no deference [should be] accorded to the FISC's probable cause determinations." *United States v. Rosen*, 447 F.Supp. 2d 538, 545 (E.D. Va. 2006). The need for de novo review is critically important if this Court declines to permit the defense participation in the suppression issues. *Id.* ("de novo review is particularly important "especially given that the review is ex parte and thus unaided by the adversarial process."); see also *United States v. Warsame*, 547 F.Supp. 2d 982, 990 (D. Minn. 2008).

Additionally, this Court must give an exacting review of the FISA materials because at this stage, the FISA activity has moved out of the realm of intelligence gathering and is being used to obtain a criminal conviction. The focus now should be the rights of the defendant against whom the government is acting, and not the interests of intelligence.

III. ACCESS TO FISA DISCOVERY IS REQUIRED TO LITIGATE SUPPRESSION ISSUES AND IS REQUIRED IN ORDER TO CONFORM WITH DUE PROCESS OF LAW.

The district court has the discretion to disclose portions of relevant materials, under appropriate protective procedures, if it decides that such disclosure is necessary to make an accurate determination of the legality of the surveillance, or is otherwise required by due process. 50 U.S.C. §§ 1806(f) (electronic surveillance), 1825(g) (physical searches); *United States v. Stewart*, 590 F.3d 93, 128 (2d Cir. 2009). This section will show that both principles require that the defense have access to the FISA materials in this case.

A. Disclosure of FISA Materials is Necessary to Accurately Determine the Legality of the FISA Surveillance and Searches.

In determining the legality of surveillance, "the court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance." 50 U.S.C. §§ 1806(f) (electronic surveillance), § 1825(g) (physical searches). Disclosure is, therefore, warranted when a court needs a defense attorney's input to decide whether to suppress evidence obtained through a FISA order.

While courts have not allowed defense participation in suppression hearings, the decisions have articulated several principles that support defense participation on Mr. Muhtorov's behalf. For example, in both *United States v. Belfield*, 692 F.2d 141, 147 (D.C. Cir. 1982), and *United States v. Ott*, 827 F.2d 473, 476 (9th Cir. 1987), the courts identified issues such as misrepresentations of fact, vague identification, or records showing over broad surveillance may require disclosure to the defense. Here, there are many potential bases for suppression based on unlawful surveillance. There are, furthermore, several complicated issues that make the defense's input necessary.

Accordingly, pursuant to 50 U.S.C. § 1806(f), the defendant asks this court to order the government to provide the following materials: All applications, extensions, orders, and related materials underlying the electronic surveillance of the defendant conducted pursuant to FISA, as well as applications for such surveillance of any third-party target which intercepted defendant.

B. Input from the Defense is necessary to make an accurate determination as to whether Mr. Muhtorov is a foreign power or agent thereof or if a "significant purpose" of the FISA application was foreign intelligence gathering.

Defense input is necessary for an accurate determination of the suppression issues raised above – that Mr. Muhtorov is not a foreign power or agent of a foreign power and that a "significant purpose" of the FISA application was not foreign intelligence gathering.

With respect to both physical searches and electronic surveillance, FISA requires that a court find probable cause to believe that the target of the investigation is a foreign power or agent of a foreign power, and that the facility or place at which the surveillance or search is directed is being used or is about to be used by the target. 50 U.S.C. §§ 1805(a)(2)(A)-(B), 1824(a)(2)(A)-(B). The FISA application here may be insufficient as to whether Mr. Muhtorov can be reasonably viewed as a foreign power or agent of a foreign power.

Section 1801(a)-(b) provides several definitions and categories of "foreign power" and "agent of a foreign power." None of those definitions apply to Mr. Muhtorov. Indeed, the only category that can even arguably apply to Mr. Muhtorov is the "agent of a foreign power" definition provided in § 1801(b)(1)(C). That definition provides that an agent of a foreign power includes a person who "engages in international terrorism or activities in preparation therefore." "International terrorism," is defined as activities that:

- (1) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a

criminal violation if committed within the jurisdiction of the United States or any State;

(2) appear to be intended-

(A) to intimidate or coerce a civilian population;

(B) to influence the policy of a government by intimidation or coercion; or

(C) to affect the conduct of a government by assassination or kidnapping; and

(3) occur totally outside the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum. 50 U.S.C. § 1801(c).

As enacted in 1978, FISA applied to interceptions the "primary purpose" of which was foreign intelligence. However, as amended in 2001 by the USA PATRIOT Act, the statute now applies to interceptions that have international intelligence gathering as a "significant purpose." See *United States v. Ning Wen*, 477 F.3d 896, 897 (7th Cir. 2007); 50 U.S.C. § 1804(a)(6)(B).

The Foreign Intelligence Surveillance Court of Review ("FISCR"), has concluded that the amended statute allows domestic use of intercepted evidence provided that a "significant" international objective is present at the time of the FISA order. *Ning Wen*, 477 F.3d at 897 (citing *Sealed Case*, 310 F.3d 717 (F.I.S.Ct.Rev.2002)). The FISCR has further stated that the "significant purpose" test, "impose[s] a requirement that the government have a measurable foreign intelligence purpose, other than just criminal

prosecution of even foreign intelligence crimes" in seeking to obtain a FISA order.

Sealed Case, 310 F.3d 717, 735 (F.I.S.Ct.Rev.2002).

This Court should not be persuaded by any argument that this was strictly a "terrorism" investigation and thus had a significant foreign intelligence objective. Thus, the mere fact that a certain investigation is in relation to "terrorism" does not establish a "significant" foreign connection under FISA.

In deciding probable cause in a search warrant context, courts are instructed to rely on common sense. *Illinois v. Gates*, 462 U.S. 213, 239 (1983). Here, common sense and objectivity shows that this was a criminal investigation from the beginning. Common sense further shows that, in this case, FISA was used as a tool to circumvent the United States Constitution and procedures in place to protect the public and defendants from government overreaching. Common sense defies how a foreign intelligence-gathering mission turns into a full-blown criminal prosecution within days. In sum, looking at the entirety of this investigation, it is obvious that its sole purpose was to build a criminal case, and had no relevance to foreign intelligence gathering. Accordingly, FISA was improperly used and the fruits of the FISA searches and surveillance should be suppressed.

These are complex issues that involve statutory interpretation and legal principles to which the defense can, and should, be able to contribute. Both arguments address issues where there is little, if any, guidance from the Tenth Circuit. And in a similar vein, few courts throughout the nation have addressed these issues. Therefore, this Court would benefit from the adversarial process ("the basic framework of the American criminal justice system") in deciding these issues. *United States v. Michelle's*

Lounge, 39 F.3d 684, 699 (7th Cir. 1994); *see also United States v. Thompson*, 827 F.2d 1254, 1259 (9th Cir. 1987) ("[a]dversary proceedings do in fact take more time, and they are more cumbersome, but with good reason: The adversary process helps us get at the truth").

Furthermore, there are issues that have not been raised as suppression issues that may very well invalidate the FISA investigation upon further analysis. These issues are addressed below.

C. Defense Involvement is Necessary to Address why the information could not be obtained by normal investigative procedures.

An important check on governmental abuse of FISA is that it may only be used when the Attorney General certifies, "that such information cannot reasonably be obtained by normal investigative procedures." 50 U.S.C. §§ 1804(a)(6)(C); 1823(a)(6)(C). A defense perspective is necessary to determine why normal investigative procedures could not be used in this case and to refute the government's explanation for why it relied on FISA.

D. Defense involvement is necessary to address questions related to minimization of government intrusion in this case.

Under FISA, as under the Title III wiretap statute, the government is required to demonstrate it has minimized its intrusions. *See* 50 U.S.C. §§ 1801(h); 1802(a)(1)(C); 1804(a)(4); 1805(a)(3); 1806(a); 1821(4); 1822(a)(1)(A)(iii); 1823(a)(4); 1824(a)(3), and (c)(2)(A); 1825(a); 1861(g); 1881a(e) and (g)(2)(A)(ii) and (i)(2)(C); 1881b(b)(D) and (c)(1)(C) and (c)(3)(C) and (d)(2); 1881c(b)(4) and (c)(1)(C) and (c)(3)(C) and (d)(2).

[The] 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. If the data is not foreign intelligence information as defined by the statute, the procedures are to ensure that the government does not use the information to identify the target or third party, unless such identification is necessary to properly understand or assess the foreign intelligence information that is collected.

In re Sealed Case, 310 F.3d at 731 (citing § 1801(h)(2)).

The statute requires three specific types of minimization to protect distinct interests. 50 U.S.C. § 1801. First, by minimizing acquisition, Congress envisioned that surveillance should be discontinued where the target is not a party to the communications. Second, by minimizing retention, Congress intended that information acquired, which is not necessary for obtaining, producing, or disseminating foreign intelligence information, be destroyed where feasible. Third, by minimizing dissemination, Congress intended that even lawfully retained information should only be divulged to those officials with a specific need. *In re Sealed Case*, 310 F.3d at 731. "The FISA minimization procedures were enacted 'generally to parallel the minimization provision in existing [electronic surveillance] law.'" *United States v. Thomson*, 752 F. Supp. 75,80 (W.D.N.Y. 1990) (quoting S. Rep. No. 95-701, at 39 (1978), reprinted in 1990 U.S.C.C.A.N. 4008).

In this case, based on the limited information known to the defense, the concern is that the surveillance was extremely overly broad, and there was little to no effort made to minimize the amount of intrusion to information related foreign intelligence gathering. In sum, this is one of those cases where defense input is necessary because there was surveillance of such a "significant amount of nonforeign intelligence

information" that it is apparent that the minimization procedures were not followed.

United States v. Belfield, 692 F.2d 141 (D.C. Cir. 1982).

E. Due Process requires disclosure of FISA material as well as any classified information to the defense.

FISA requires disclosure "to the extent that due process requires discovery or disclosure." 18 U.S.C. §§ 1806(g), 1825(h), 1845(g)(2). In the contest between disclosure of state secrets and the defendant's right to a fair trial, the latter wins out. As the Supreme Court has long recognized, "the Government can invoke its evidentiary privileges only at the price of letting the defendant go free . . . it is unconscionable to allow [the Government] to under take prosecution and then invoke its governmental privileges to deprive the accused of anything which might be material to his defense." *United States v. Reynolds*, 345 U.S. 1, 12 (1953). This principal has remained unchanged over time. In fact, the Second Circuit recently reiterated that in a criminal prosecution the defense must have access to information that is "helpful or material" to the defense, regardless of whether such information is a state secret. *United States v. Aref*, 533 F.3d 72, 80 (2d Cir. 2008). Being "helpful or material" does not necessarily rise to the level of the government's obligations under *Brady v. Maryland*, 373 U.S. 83 (1963), because "information can be helpful without being favorable in the Brady sense." *Id.* Thus, the government must disclose any and all helpful information to the defense, regardless of whether it is classified. *Id.*; see also *United States v. Varca*, 896 F.2d 900, 905 (5th Cir. 1990).

Moreover, the government is given four options in a case that involves classified information that is material to the defense, in accordance with the procedures defined

by the Classified Information Procedures Act (CIPA). In such a case, the government can either: (1) disclose the material to counsel; (2) declassify the material and disclose it; (3) in some circumstances, provide an unclassified summary of the material; or (4) if it refuses any of the three disclosure options, it faces exclusion of the evidence or dismissal of its case. 18 U.S.C. app. III at § 6(c) and (e). In a case such as this, where state secrets are expected to be elicited from the government, the proper procedure is to follow CIPA rather than to preclude discovery and examination of materials by the defense. *See, e.g., United States v. Poindexter*, 732 F.Supp. 142, 154-55 (D.D.C. 1990).

The importance of a defense perspective in assessing the materials in this case that are helpful to Mr. Muhtorov's defense cannot be overstated. The defense will provide a unique position to evaluate the plethora of electronic surveillance present in this case and assess its helpfulness to Mr. Muhtorov. *Alderman v. United States*, 394 U.S. 165, 182-84 (1969). In *Alderman*, the Supreme Court recognized that "the need for adversary inquiry is increased by the complexity of the issues presented for adjudication, and by the consequent inadequacy of ex parte procedures as a means for their accurate resolution, the displacement of well-informed advocacy necessarily becomes less justifiable." *Id.* at 183-84. The Court recognized that a district court's ability to represent the interests of a defendant is limited by the fact that

[a]n apparently innocent phrase, a chance remark, a reference to what appears to be a neutral person or event, the identity of a caller or the individual on the other end of a telephone, or even the manner of speaking or using words

may have special significance to one who knows the more intimate facts of an accused's life.

Alderman, 394 U.S. at 182. In this case, "the volume of the material to be examined and the complexity and difficulty of the judgments involved" requires a defense perspective and the protections provided by the adversarial process. *Id.* at 182 n.14.

Finally, it must be noted that if the Court declines to permit the defense its due process right to access the FISA information to determine its helpfulness, the Court must "err on the side of protecting the interests of the Defendant," in deciding what is to be disclosed, again because of the ex parte nature of FISA proceedings are not adequate to protect defendants. *United States v. Hanjuan Jin*, 791 F.Supp.2d 612, 620 (N.D.Ill. 2011).

IV. FISA IS UNCONSTITUTIONAL.

Although a number of the challenges raised here have been rejected by other courts both before and after the Patriot Act Amendments to FISA in 2001, the Court should consider the claims in light of the facts of this case, amendments to the Patriot Act, and the lack of Supreme Court and Tenth Circuit authority addressing FISA issues.

A. The "Significant Purpose" Standard Violates the Fourth Amendment's Prohibition on Unreasonable Searches and Seizures.

Before FISA was enacted, and for the first 25 years of its existence, the "primary purpose" for surveillance or searches was required to be intelligence gathering. *United States v. Truong Dinh Hung*, 629 F.2d 908, 912-13 (4th Cir. 1980). The non-criminal purpose standard was essential to the cases upholding FISA's constitutionality. In the Patriot Act of 2001 and a subsequent decision of the FISC, the primary purpose test

was abandoned. The change requires reconsideration of FISA's constitutionality given the use of FISA for normal criminal purposes for governmental intrusions, which implicate the Fourth, Fifth, and Sixth Amendments.

1. The "primary purpose" standard was essential to the Constitutionality of FISA.

Prior to the amendments to FISA pursuant to the Patriot Act in 2001, information obtained pursuant to a FISA investigation could be used in a criminal proceeding only if the "primary purpose" of the FISA investigation was foreign intelligence gathering. *United States v. Duggan*, 743 F.2d 59, 77 (2d Cir. 1984). Critically important, this "primary purpose" standard arose from pre-FISA case law 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"); *United States v. Brown*, 484 F.2d 418, 427 (5th Cir. 1973) ("The serious step of recognizing the legality of a warrantless wiretap can be justified only when, as in the case before us, the foreign and sensitive nature of the government surveillance is crystal clear.") (Goldberg, J., concurring). Because each of these cases either predates FISA or addresses searches that predated FISA, logically speaking, the "primary purpose" restriction arose from

Constitutional, rather than statutory interpretation, concerns. Indeed, as the Fourth Circuit made clear:

[T]he executive can proceed without a warrant only if it is attempting primarily to obtain foreign intelligence from foreign powers or their assistants. We think that the unique role of the executive in foreign affairs and the separation of powers will not permit this court to allow the executive less on the facts of this case, but we also are convinced that the Fourth Amendment will not permit us to grant the executive branch more.

Truong, 629 F.2d at 916.

2. FISA's original language.

As initially enacted, in 1978, FISA required that "the purpose of the surveillance is to obtain foreign intelligence information." However, in order to comply with the Constitution, courts interpreted this language as requiring that the "primary purpose" of a FISA investigation to be directed at obtaining foreign intelligence information. *United States v. Johnson*, 952 F.2d 565, 572 (1st Cir. 1991); *United States v. Pelton*, 835 F.2d 1067, 1074-76 (4th Cir. 1987). This test "ensured that law enforcement officials availed themselves of FISA's more flexible certification procedures only if they primarily sought to obtain foreign intelligence information." *United States v. Warsame*, 547 F.Supp. 2d 982, 995 (D. Minn. 2008). In other words, it was essential to the constitutionality of FISA.

3. The "significant purpose" standard violates the Fourth Amendment on its face and as applied in this case.

This "primary purpose" test – which has its basis in the Constitution - was the FISA procedure until 2001 when the Patriot Act 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). As the FISC has noted, the government advocated for this amendment to FISA, whereby the article "the" was replaced with the article "a" before the word "purpose," "in order to avoid the requirement of meeting the 'primary purpose' test." *In re Sealed Case*, 310 F.3d at 732.

Under the new "significant purpose" test, as interpreted by the FISC, the government can obtain a FISA warrant provided that it has some "measurable foreign intelligence purpose, other than just criminal prosecution," in order to obtain a FISA warrant. *Id.* at 735. The test is satisfied, "[s]o long as the government entertains a realistic option of dealing with the agent other than through criminal prosecution." *Id.* at 735. The standard, as other courts have recognized, problematically seems to allow FISA surveillance where the primary purpose is criminal prosecution. See, e.g., *Warsame*, 547 F.Supp. 2d at 998. This standard cannot withstand a Fourth Amendment challenge.

As shown above, the "primary purpose" test is based on the Constitution and pre-dates FISA. As the Fourth Circuit stated, the primary purpose test is as far as the Fourth Amendment will permit the Government to go in being permitted to physically search and electronically monitor an individual without a warrant. *Truong*, 629 F.2d at 916. Logically, then, the "significant purpose" test, which permits the government to obtain authority to physically search and electronically monitor an individual without a

warrant and with the primary purpose of criminally prosecuting them, *In re Sealed Case*, 310 F.3d at 732, is unconstitutional.

The inherent danger in FISA's significant purpose test is that, in a wide range of criminal investigations, the government can now effect an end-run around the Fourth Amendment merely by asserting a desire to gather foreign intelligence information from the person it in fact intends to prosecute. This has prompted one court to hold that FISA is unconstitutional. *Mayfield v. United States*, 504 F.Supp.2d 1023, 1038 (D.Or. 2007), rev'd on other grounds, 599 F.3d 964 (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"). And the same basis led to another court to having "very significant concerns that the 'significant purpose' standard violates the Fourth Amendment." *Warsame*, 547 F.Supp. 2d at 998 (but declining to reach the issue because, on the case before it, the FISA investigation satisfied the primary purpose test).

The "significant purpose" test, therefore, renders FISA unconstitutional on its face and as applied in this case. It is unconstitutional on its face because under the "significant purpose" test, every FISA surveillance order empowers the government to disregard the Fourth Amendment even if its primary purpose is to gather evidence of a crime. In addition, every FISA order fails to satisfy several of the Fourth Amendment's requirements – the orders do not qualify as warrants, fail to require probable cause, fail the particularity requirement because of their lengthy duration, and provide inadequate notice. See *United States v. Salerno*, 481 U.S. 739, 745 (1987) (a statute is

unconstitutional on its face when "no set of circumstances exists under which the Act would be valid").

The significant purpose test, furthermore, renders FISA unconstitutional as applied in this case because the investigation of Mr. Muhtorov was at least primarily, if not fully, criminal. Mr. Muhtorov operated exclusively within the United States and there is no apparent foreign intelligence gathering connection. The FISA application in this case, therefore, must have relied on the "significant purpose" test, and would not have been upheld under the former "primary purpose" test. Accordingly, this Court should rule that the FISA "significant purpose" standard as applied in this case is unconstitutional.

B. FISA Violates Numerous Other Fourth Amendment Protections.

1. FISA Authorizes Warrants Without the Meaningful Judicial Review Required Under The Fourth Amendment.

In order to conduct a search or surveillance in an ordinary criminal investigation, the government must obtain the prior authorization of a neutral, disinterested magistrate who has the authority to determine whether the requirements of Rule 41 or Title III have been satisfied. See FED. R. CRIM. P. 41 (governing physical searches in criminal investigations); 18 U.S.C. §§ 2518(1)(b), (2) & (3) (governing electronic surveillance in criminal investigations); see *Johnson v. United States*, 333 U.S. 10, 13-14 (1948) ("The point of the Fourth Amendment, which often is not grasped by zealous officers, is not that it denies law enforcement the support of the usual inferences which reasonable men draw from evidence. Its protection consists in requiring that those inferences be

drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime.").

FISA reduces the authority of judges reviewing warrants issued under its provisions. The FISC does not have full authority to determine whether, in any particular investigation, the FBI has satisfied the requirements of FISA. The government satisfies most of FISA's requirements simply by certifying that the requirements are met. See 50 U.S.C. § 1804(a)(6); 1823(a)(6) (enumerating necessary certifications).

While certain (but not all) of these certifications must be accompanied by "a statement of the basis for the certification," 50 U.S.C. § 1804(a)(6)(E), the statute makes clear that the FISA court is not to fully scrutinize such statements, but rather is to defer to the government's certification unless it is "clearly erroneous on the basis of the statement made under § 1804(a)(6)(E)." 18 U.S.C. § 1805(a)(4). As the FISC has acknowledged, "this standard of review is not, of course, comparable to a probable cause finding by the judge." *In re Sealed Case*, 310 F.3d at 739 (quoting H. R. REP. NO. 95-1283, at 80 (1978)). Prior to the Patriot Act Amendment, it may have been reasonable to limit judicial review of warrant applications. Once, however, the use of warrants was permitted even when the "primary purpose" was no longer intelligence gathering, the rationale for limiting the judiciary's role can no longer stand under the Fourth Amendment. The protections of the people's right against government intrusions for criminal investigatory purposes required by the Fourth Amendment must be present if the government is to use evidence in a criminal prosecution. "A search prosecuted in violation of the Constitution is not made lawful by what it brings to light;

and the doctrine has never been recognized by this court, nor can it be tolerated under our constitutional system, that evidences of crime discovered by a federal officer in making a search without lawful warrant may be used against the victim of the unlawful search where a timely challenge has been interposed." *Byars v. United States*, 273 U.S. 28, 29-30 (1927).

Since surveillance and searches conducted pursuant to FISA here were likely conducted without meaningful prior judicial review, they were unreasonable under the Fourth Amendment.

2. FISA Orders Do Not Qualify as Warrants Under the Fourth Amendment.

FISC surveillance orders are not warrants within the meaning of the Fourth Amendment. See *In re Sealed Case*, 310 F.3d at 741 (acknowledging that FISA orders "may not be . . . 'warrant[s]' contemplated by the Fourth Amendment"). The Supreme Court has held that a warrant must be issued by a neutral, detached magistrate; must be based on a demonstration of probable cause; must relate to a particular offense; and must particularly describe the things to be seized as well as the place to be searched. *Dalia v. United States*, 441 U.S. 238, 255 (1979). FISC orders do not satisfy these requirements.

On the contrary, and as clearly demonstrated by this case, FISA empowers the government to conduct the most intrusive kinds of surveillance with lesser judicial review than required by the Constitution, without showing criminal probable cause, and without meeting particularity requirements. Because FISC orders are not warrants, searches conducted under FISA are presumptively unreasonable. See, e.g., *Payton v.*

New York, 445 U.S. 573, 586 (1980); *Chimel v. California*, 395 U.S. 752, 762-63 (1969). The surveillance at issue in this case cannot overcome that presumption.

3. FISA Warrants Do Not Satisfy The Particularity Requirement.

The electronic surveillance and searches in this case were substantial. As the Complaint Affidavit indicates, Mr. Muhtorov's home was searched on at least two occasions, his email account was searched, his personal journals were searched, and his computer files were searched. The duration and scope of these intrusions, obviously, was not strictly limited. Such surveillance violated the Fourth Amendment's particularity requirement.

The Fourth Amendment ordinarily prohibits the government from conducting intrusive surveillance unless it first obtains a warrant describing with particularity the things to be seized as well as the place to be searched. *Berger v. New York*, 388 U.S. 41, 58 (1967) (noting that Fourth Amendment particularity requirement was intended to prevent the government's reliance on "general warrants" that allow "the seizure of one thing under a warrant describing another"). In *Berger*, the Supreme Court stated that the importance of the particularity requirement "is especially great in the case of eavesdropping." *Id.* at 56. The Court explained: "[B]y its very nature eavesdropping involves an intrusion on privacy that is broad in scope." *Id.* "[T]he indiscriminate use of such devices in law enforcement raises grave constitutional questions under the Fourth and Fifth Amendments, and imposes a heavier responsibility on this Court in its supervision of the fairness of procedures." *Id.*

With respect to eavesdropping devices and wiretaps, the particularity requirement demands not simply that the government describe in detail the communications it intends to intercept, but also that the duration of the intercept be strictly limited. See *Berger*, 388 U.S. at 58-60. Title III, which Congress enacted shortly after *Berger* was decided, limits the term of surveillance orders to 30 days. 18 U.S.C. § 2518(5). FISA, by contrast, authorizes surveillance terms of up to 90 or 120 days or even one year. 50 U.S.C. § 1805(d)(1); 1824(d)(1). To the extent FISA is read to permit issuance of a warrant - or an extension - without the type of particularity required under Title III, it would violate the Constitution. But see *Mubayyid*, 521 F. Supp. 2d at 138.

4. Surveillance was Conducted Without Compliance with the Fourth Amendment's Probable Cause Requirement.

The Fourth Amendment ordinarily prohibits the government from conducting intrusive surveillance without first demonstrating criminal probable cause - probable cause to believe that "the evidence sought will aid in a particular apprehension or conviction for a particular offense." See *Dalia*, 441 U.S. at 255. Although the government's primary purpose in this case was to obtain evidence of criminal activity, it failed to satisfy the criminal probable cause requirement.

FISA authorizes the government to conduct intrusive surveillance if it can show what is known as "foreign intelligence probable cause" – probable cause to believe that the surveillance target is a foreign power or agent of a foreign power. See 50 U.S.C. § 1805(a)(3)(A). The statute does not require the government to advance any reason whatsoever – let alone probable cause – to believe that its surveillance will yield

information about a particular criminal offense. Indeed, foreign-intelligence probable cause bears only a passing resemblance to criminal probable cause. In response to a Freedom of Information Act request filed by the ACLU and others in August 2002, the FBI released, among other things, a document from the FBI's National Security Law Unit entitled, "What do I have to do to get a FISA?" The document states, in relevant part:

Probable cause in the FISA context is similar to, but not the same as, probable cause in criminal cases. Where a U.S. person is believed to be an agent of a foreign power, there must be probable cause to believe that he is engaged in certain activities, for or on behalf of a foreign power, which activities involve or may involve a violation of U.S. criminal law. The phrase "involve or may involve" indicates that the showing of [nexus to] criminality does not apply to FISA applications in the same way it does to ordinary criminal cases. As a result, there is no showing or finding that a crime has been or is being committed, as in the case of a search or seizure for law enforcement purposes. The activity identified by the government in the FISA context may not yet involve criminality, but if a reasonable person would believe that such activity is likely to lead to illegal activities, that would suffice. In addition, and with respect to the nexus to criminality required by the definitions of "agent of a foreign power," the government need not show probable cause as to each and every element of the crime involved or about to be involved.

"What do I have to do to get a FISA?," at 2 (Document released by FBI in response to August 21 Freedom of Information Act request submitted by ACLU et al.).

It is clear that foreign-intelligence probable cause is not "probable cause" within the ordinary meaning of the Fourth Amendment. The surveillance at issue in this case was not premised on criminal probable cause and accordingly was unreasonable within the meaning of the Fourth Amendment.

C. The Ex Parte, In Camera FISA Process Violates Due Process, A Defendant's Rights To Be Present At All Critical Stages Of The Criminal Process, And His Right To The Effective Assistance Of Counsel.

FISA authorizes the unprecedented exclusion of the accused from critical stages of the prosecution, including review of the motion to suppress evidence. The post-indictment procedure, in a criminal prosecution, is conducted ex parte and in camera and without the defendant ever having the right to even see the warrants or affidavits he is challenging. To permit Muhtorov's motion to proceed in this manner would violate his Fifth and Sixth Amendment rights. Fundamental to due process is the right to notice and an opportunity to be heard. *See LaChance v. Erickson*, 522 U.S. 262 (1998). The interest at stake is the most fundamental liberty- freedom from incarceration. *Turner v. Rogers*, 131 S.Ct. 2507, 2518 (2011) ("Freedom 'from bodily restraint' lies 'at the core of the liberty protected by the Due Process Clause.'"). Equally fundamental is a defendant's right to be present at, and participate in, all critical stages of a criminal prosecution and to be meaningfully assisted by counsel. *See Montejo v. Louisiana*, 129 S. Ct. 2079, 2085 (2009); *Tennessee v. Lane*, 541 U.S. 509, 523 (2004).

To be sure, the Constitution recognizes some limits on a defendant's participation in the criminal process. The government may secure an indictment without his participation. *United States v. Salsedo*, 607 F.2d 318, 319 (9th Cir. 1979). In limited circumstances, the court may review potential evidence ex parte to determine whether it is material to the defense. *United States v. Mejia*, 448 F.3d 436, 543-54

(D.C. Cir. 2006). If it, it must be disclosed or the government loses the opportunity to use it. *Skinner v. Switzer*, 131 S. Ct. 1289, 1300 (2011) (citing *Brady*, 373 U.S. at 87).

The FISA limitations on a defendant's participation are different in kind, allowing the court to determine complex constitutional questions in a non-adversarial setting and in secret. The Constitution forbids such a process, as analogous holdings show.

The unconstitutionality of the type of process authorized by FISA is supported by *United States v. Abuhamra*, 389 F.3d 309 (2d Cir. 2004). There, in the context of a bail application, the government submitted – and the District Court considered – evidence ex parte and in camera. The Court rejected one-sided secret proceedings: “Particularly where liberty is at stake, due process demands that the individual and the government each be afforded the opportunity not only to advance their respective positions but to correct or contradict arguments or evidence offered by the other.” *Id.* at 322. *Abuhamra* also noted that such a procedure not only violated the defendant's due process rights but also the right of public access to criminal trials. *Id.* at 316 n.3, 323; see also *Alderman*, 394 U.S. at 182-84. FISA's ex parte, in camera process, whatever its legality in the context of foreign surveillance, cannot constitutionally displace the defendant's rights under the Fifth and Sixth Amendments. See *United States v. Coplon*, 185 F.2d 629, 638 (2d Cir. 1950) (finding the refusal to allow the defense to see records the judge reviewed in camera to determine if the “taps” led to evidence introduced at trial violated the defendants' constitutional right). “Few weapons in the arsenal of freedom are more useful than the power to compel a government to disclose

the evidence on which it seeks to forfeit the liberty of its citizens." *Coplon*, 185 F.2d at 638.

One of the first cases to consider these arguments under FISA was *Belfield*. There, the court rejected similar Fifth and Sixth Amendment claims. 692 F.2d at 148. The court's reasoning was, however, anchored in the fact that "FISA is concerned with foreign intelligence surveillance." *Id.* Courts that rejected similar claims after the Patriot Act amendments have failed to recognize the change in the statutory criteria. See, e.g., *United States v. Kashmiri*, No.09 CR 830-4, 2010 WL 4705159 (N.D. Ill. 2010). Once Congress expanded the purposes of and standards for surveillance, it shifted the constitutional calculus. As stated in *Boumediene v. Bush*, 553 U.S. 723, 797 (2008), "security subsists, too, in fidelity to freedom's first principles." Those principles support the conclusion that FISA no longer passes constitutional muster if it shuts criminal defendants out of the process.

D. The FISA "Suppression" Process Unconstitutionally Interferes With The Article III Judicial Power.

Chief Justice John Marshall in *Cohens v. Virginia*, noted that the judicial power of the federal courts "extends to all cases arising under the constitution or a law of the United States, whoever may be the parties." 19 U.S. (6 Wheat.) 264, 392 (1821). FISA may trigger this judicial power, but it cannot constitutionally expand or restrict the scope of Article III. It does both.

In considering the constitutionality of FISA's limit on judicial power, "[t]he controlling question is whether the function to be exercised by the court is a judicial function." *Fed. Radio Comm'n v. Nelson Bros., Co.*, 289 U.S. 266, 277 (1933). An

Article III court determining a Fourth Amendment suppression motion on a federal indictment surely performs a "judicial function."

The first defect in FISA under Article III is that it permits the courts to act when there is no case or controversy. *Camreta v. Green*, 131 S. Ct. 2020, 2028 (2011) ("Article III of the Constitution grants this Court authority to adjudicate legal disputes only in the context of "Cases" and "Controversies."). The role of the courts is to resolve disputes between or among parties. *Principal Life Ins. Co. v. Robinson*, 394 F.3d 665, 671 (9th Cir. 2005). They may not issue advisory opinions. *Sierra Club v. Morton*, 405 U.S. 727, 732 n.3 (1972). Contrary to these principles, FISA permits the courts to act in a one-sided manner, treating the question of suppression as if only one party had an interest sufficient to warrant judicial action.

The second defect in FISA is that it limits the Judiciary's Article III powers by requiring the courts to defer to executive assertions in a criminal case. 50 U.S.C. §§ 1805(a)(4), 1824(a)(4). The fact that FISA gives the Attorney General undue control of the warrant and suppression motion processes and limits FISA review infringes on the judicial responsibility to say what the law is, as it "is a responsibility of this Court as ultimate interpreter of the Constitution." *Baker v. Carr*, 396 U.S. 186, at 211 (1962). *See Kendall v. United States*, 37 U.S. 524, at 526 (1838) (discerning judicial authority and separation of powers).

The third defect is that FISA, as implemented ex parte and in camera, violates the separation of powers inherent in the first three Articles of the Constitution. While the Executive Branch must assure that the laws are faithfully executed, the Judiciary

ultimately must decide whether the executive action complies with legislative standards. By conferring deference to the Executive while excluding the citizen, the separation of powers is breached, with the citizen ineffectively protected from executive overreaching.

The judicial power to conduct a Fourth Amendment suppression hearing flows directly from Article III of the Constitution. It does not flow from, nor can it be limited by, a purported congressional delegation to the Attorney General, who in turn tells this Court how to exercise its judicial powers and discretion in a bona fide constitutional "case and controversy."

V. CONCLUSION

First, even without FISA disclosure it is apparent that the FISA investigation in this case did not meet statutory standards. The purpose of this FISA investigation was to conduct a criminal investigation and there was no connection, much less the "significant" connection required, to foreign intelligence gathering. Furthermore, there was no probable cause to find that Mr. Muhtorov was an "agent of a foreign power" as required by FISA. Second, is that disclosure of the FISA evidence is required in this case both because defense input is necessary to properly address the complex matters at issue in the motion to suppress, and because disclosure is required under due

process principles. Finally, FISA is unconstitutional both on its face and as applied in this case because it violates the Fourth, Fifth, and Sixth Amendments, as well as Article III to the United States Constitution.

Respectfully submitted,

RAYMOND P. MOORE
Federal Public Defender

s/ Brian R. Leedy
BRIAN R. LEEDY
Assistant Federal Public Defender
633 Seventeenth Street, Suite 1000
Denver, Colorado 80202
Telephone: (303) 294-7002
FAX: (303) 294-1192
Brian.Leedy@fd.org
Attorney for Defendant

CERTIFICATE OF SERVICE

I hereby certify that on May 25, 2012, I electronically filed the foregoing

**MOTION TO SUPPRESS FISA ACQUIRED
EVIDENCE (SUPPLEMENT TO DOC. 14)**

with the Clerk of Court using the CM/ECF system which will send notification of such filing to the following e-mail addresses:

Gregory A. Holloway
Assistant U.S. Attorney
Email: gregory.holloway@usdoj.gov

David B. Savitz
Email: savmaster@aol.com

and I hereby certify that I have mailed or served the document or paper to the following non CM/ECF participant in the manner (mail, hand-delivery, etc.) indicated by the non-participant's name:

s/ Brian R. Leedy

BRIAN R. LEEDY
Assistant Federal Public Defender
633 Seventeenth Street, Suite 1000
Denver, Colorado 80202
Telephone: (303) 294-7002
FAX: (303) 294-1192
Brian.Leedy@fd.org
Attorney for Defendant