**IN THE UNITED STATES DISTRICT COURT**
**FOR THE NORTHERN DISTRICT OF ILLINOIS**
**EASTERN DIVISION**

| | |
|---|---|
| **UNITED STATES OF AMERICA,**<br><br>**Plaintiff,**<br><br>**v.**<br><br>**ILYAS KASHMIRI, *et al.*,**<br>**(Tahawwur Hussain Rana)**<br><br>**Defendants.** | **Case No. 09 CR 830-4**<br><br>**Hon. Harry D. Leinenweber** |

**MEMORANDUM OPINION AND ORDER**

## I. BACKGROUND

The November 2008 terrorist attacks in Mumbai, India, by *Lashkar e Tayyiba*, which targeted hotels, restaurants, train stations, and other public locations in the city, took the lives of more than 160 people, including six United States nationals. The United States Secretary of State has designated the Pakistan-based *Lashkar*, which has a primary objective to separate portions of the States of Jammu and Kashmir from India, as a foreign terrorist organization under Section 219 of the Immigration and Nationality Act. *See* 8 U.S.C. § 1189 (2006).

On October 18, 2009, the United States Government (the "Government") arrested Defendant Tahawwur Hussain Rana (the "Defendant"). He allegedly owned the immigration services business

First World Immigration Services, which was based out of Chicago and also had offices in New York and Toronto. The Pakistan-born Canadian citizen, who primarily lives in Chicago, has been charged with three counts. The first count is for conspiring with others to provide material support to the Mumbai attacks. Second, the government has charged Rana with providing material support to an allegedly planned terrorist attack in Denmark. This planned attack targeted the facilities of a Danish newspaper and at least two of its employees, in response to a series of cartoons published in September 2005 that depicted the Muslim prophet Mohammed. Third, Defendant has been charged with providing material support to *Lashkar*. All three counts are brought pursuant to 18 U.S.C. § 2339(A) for providing material support to terrorists.

On October 18, 2009, the United States Attorney General filed notice indicating that in its case against Defendant it intended to use evidence obtained through both physical searches and electronic surveillance pursuant to the Foreign Intelligence Surveillance Act of 1978 ("FISA"), 50 U.S.C. § 1801 *et seq*. On May 10, 2010, Defendant moved, under FISA, the due process provisions of the Fifth Amendment, the assistance of counsel provision of the Sixth Amendment, and *Brady v. Maryland*, 372 U.S. 83 (1963), that the Court order the Government to provide Defendant with all FISA applications, orders, and related documents where Defendant has been a target of electronic surveillance or a physical search. On

August 27, 2010, Defendant moved, pursuant to the Fourth and Fifth Amendments to the Constitution, and 50 U.S.C. § 1806(e), to suppress FISA electronic surveillance evidence, as well as to request a *Franks* hearing pursuant to *Franks v. Delaware*, 438 U.S. 154 (1978). The Government subsequently indicated that it would not use FISA evidence obtained by physical search in its case, and on September 22, 2010, the Court granted Defendant's Motion to Withdraw its motion to suppress evidence obtained by physical search. The Court addresses the still pending motions in this Opinion.

## II. REVIEW STANDARD FOR FISA MATERIALS

As later described in more detail, specific procedures exist for a district court to conduct an *in camera*, *ex parte* review of FISA material when it considers a motion to disclose or a motion to suppress evidence. *See* 50 U.S.C. § 1806(f). The court reviews FISA electronic surveillance materials in the same manner as the Foreign Intelligence Surveillance Court ("FISC") reviews the materials, in that it does not second-guess the Executive Branch's certification that the surveillance has a foreign intelligence objective. *In re Grand Jury Proceedings of the Special April 2002 Grand Jury*, 347 F.3d 197, 204-05 (7th Cir. 2003). The court conducts a *de novo* review of the FISA materials to determine if the electronic surveillance authorization was based upon appropriate

probable cause. *United States v. Hammond*, 381 F.3d 316, 332 (4th Cir. 2004), *vacated on other grounds*, 543 U.S. 1097 (2005).

## III. ANALYSIS

### A. Motion for Disclosure of FISA Materials

Under 50 U.S.C. § 1806(e), Defendant has standing to move to suppress evidence obtained through electronic surveillance under FISA on the grounds that it was unlawfully obtained or not made in conformity with the FISA order of authorization or approval. This provision also gives standing to an "aggrieved person" against whom FISA evidence has been obtained or derived to move to disclose this evidence. *See, United States v. Warsame*, 547 F.Supp.2d 982, 986 (D. Minn. 2008).

Defendant requests disclosure of FISA materials to assess whether to move for suppression of any evidence or information obtained under FISA. As the Second Circuit has explained, the procedure the district court follows in such a situation is an *ex parte* and *in camera* review:

> Section 1806(f) of FISA provides for *in camera, ex parte* review of the documents where the Attorney General has filed an affidavit stating that disclosure of the FISA applications and orders would harm the national security of the United States. The judge has the discretion to disclose portions of the documents, under appropriate protective procedures, only if he decides that such disclosure is "necessary to make an accurate determination of the legality of the surveillance." 50 U.S.C. § 1806(f). Such a need might arise if the judge's initial review

> revealed potential irregularities such as "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." Senate Report 95-604, at 58, *reprinted in* 1978 U.S. Code Cong. & Ad. News 3904, 3960. In general, however, "*ex parte, in camera* determination is to be the rule."

*United States v. Duggan*, 743 F.2d 59, 78 (2d Cir. 1984).

If disclosure of the FISA materials is not necessary for the district court to make an accurate determination of the legality the collection, disclosure *may not be ordered*. *See* 50 U.S.C. § 1806(f). In reviewing a FISA application, a FISA judge, whose orders the district court must review, must (1) find probable cause to believe that the target of the requested surveillance is an agent of a foreign power; (2) find that the application is complete and in proper form; and (3) when the target is a United States person, find that the certifications are not "clearly erroneous." *See Duggan*, 743 F.2d at 77. Again, this Court conducts the same review of the evidence as the FISA court undertook.

The Court has therefore conducted an *in camera* and *ex parte* review of the FISA materials related to this case. The Court finds that all of the FISA orders and applications concerning Defendant meet the standards set forth in 50 U.S.C. § 1801 *et seq.* and that the Government made a "good faith" effort in minimizing information concerning United States persons that may have been acquired

through such electronic surveillance. Therefore, the FISA electronic surveillance at issue was lawfully authorized and legally conducted.

In 2003, the Seventh Circuit wrote that it could not locate one case in which a court conducted a review of FISA materials other than through an *in camera* and *ex parte* process. *Grand Jury Proceedings*, 347 F.3d at 203. The appellant in the 2003 case argued that his was the one-in-a-million case in which such an exception should occur, and that the court should allow him to review the materials. *Id.* The court disagreed. *Id.* Subsequently, since 2003, as Defendant acknowledges, this one-in-a-million case has yet to occur. A court has never permitted defense counsel to review FISA materials. Likewise, in this case, because disclosure of the materials is unnecessary for the Court to determine the legality of the collection, Defendant's Motion for Disclosure is denied. *See* 50 U.S.C. § 1806(f).

**B. Motion to Suppress FISA Materials**

In his Motion to Suppress the FISA materials, Defendant argues that FISA, as it exists after the passage of the Patriot Act in 2001, violates the Fourth Amendment. This argument has been made before several other courts, which have almost unanimously rejected it. *See United States v. Ning Wen*, 477 F.3d 896, 897 (7th Cir. 2007); *United States v. Damrah*, 412 F.3d 618, 625 (6th Cir. 2005); *United States v. Abu-Jihaad*, 531 F.Supp.2d 299, 309 (D. Conn.

2008); *Warsame*, 547 F.Supp.2d at 993; *United States v. Mubayyid*, 521 F.Supp.2d 125, 139-40 (D. Mass 2007); *United States v. Holy Land Found. for Relief and Dev.*, No. 04-CR-240-G, 2007 WL 2011319, at *6 (N.D. Tex. July 11, 2007).

The Court is not persuaded by the one outlier district court case which held that FISA, as it currently exists, violates the Fourth Amendment. *Mayfield v. United States*, 504 F.Supp.2d 1023, 1042-43 (D. Or. 2007), *vacated*, 588 F.3d 1252 (9th Cir. 2009), *vacated and superseded*, 599 F.3d 964 (9th Cir. 2010) (holding that plaintiff lacked standing to seek declaratory relief against the United States and declining to address the Fourth Amendment issue). Plus, this Court must follow the Seventh Circuit's *Ning Wen* decision in analyzing FISA's constitutionality.

The primary issue Defendant raises concerning the constitutionality of FISA is that after the terrorist attacks of September 11, 2001, law enforcement has used FISA as a tool to gather evidence for criminal prosecutions, rather than to obtain foreign intelligence information. The probable cause necessary to obtain a FISA order differs from that of a traditional search warrant. To obtain a FISA order, 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 is directed is being used, or is about to be used, by a foreign power or an agent of a

foreign power." 50 U.S.C. § 1804(a)(4). No requirement exists to show probable cause of presently occurring or past criminal activity, which is necessary for a search warrant. *See Brinegar v. United States*, 338 U.S. 160, 175-76 (1949) ("Probable cause exists where the facts and circumstances within . . . [the officers'] knowledge and of which they had reasonably trustworthy information [are] sufficient in themselves to warrant a man of reasonable caution in the belief that an offense has been or is being committed.") (internal quotation omitted).

The Foreign Intelligence Surveillance Court of Review ("FISCR") addressed the issue of FISA's post-Patriot Act constitutionality in *In re Sealed Case*, 310 F.3d 717 (FISA Ct. Rev. 2002). As originally passed in 1978, FISA provided a tool to gather foreign intelligence information through electronic surveillance of a foreign power or an agent of a foreign power. *Id.* at 722-23. Congress amended FISA in 1994 to also cover physical searches. *Id.* at 722 n.7. In the 1980s, the Justice Department interpreted FISA "as limiting the Department's ability to obtain FISA orders if it intended to prosecute the targeted agents — even for foreign intelligence crimes" such as international terrorism or sabotage. *Id.* at 723. The FISCR found this interpretation "puzzling." *Id.* The court interpreted the statute as reading that while "the purpose" of the FISA order — as certified by a national security official in the Executive Branch

— had to be to obtain foreign intelligence information, "FISA as passed by Congress in 1978 clearly did *not* preclude or limit the government's use or proposed use or foreign intelligence information, which included evidence of certain kinds of criminal activity, in a criminal prosecution." *Id.* at 727 (emphasis in original).

Nevertheless, in 1995 the U.S. Attorney General adopted "Procedures for Contacts Between the FBI and the Criminal Division Concerning Foreign Intelligence and Foreign Counterintelligence Investigation." *Id.* These procedures, instituted to comply with the "primary purpose" test that some courts had used in ruling on the admissibility of FISA evidence, in practice created a "wall" that prevented FBI intelligence officials from communicating with the Criminal Division in cases that involved FISA surveillance. *Id.* at 727–28.

The Patriot Act attempted to break down this wall. In particular, it changed the language of 50 U.S.C. § 1804(a)(7)(B)—part of the rules governing the certification process for a FISA order — from "*the purpose* of the surveillance is to obtain foreign intelligence information" to "*a significant purpose* of the surveillance is to obtain foreign intelligence information." *Id.* at 729–29 (emphasis added). Through this seemingly minor amendment to FISA, "Congress was keenly aware that [it] relaxed a requirement that the government show that its

primary purpose was other than criminal prosecution." *Id.* at 732. Significantly, the government could obtain a FISA order even if the purpose of the surveillance was to obtain information concerning criminal activity, as long as the government also presented as part of its FISA application a significant foreign intelligence purpose for the surveillance. As the *Sealed Case* decision explained:

> [T]he Patriot Act amendment, by using the word "significant," eliminated any justification for the FISA court to balance the relative weight the government places on criminal prosecution as compared to other counterintelligence responses. If the certification of the application's purpose articulates a broader objective than criminal prosecution—such as stopping an ongoing conspiracy—and includes other potential non-prosecutorial responses, the government meets the statutory test. Of course, if the court concluded that the government's sole objective was merely to gain evidence of past criminal conduct—even foreign intelligence crimes—to punish the agent rather than halt ongoing espionage or terrorist activity, the application should be denied.

*Id.* at 735.

In addressing *Sealed Case*, the Seventh Circuit wrote that it "concluded that the amended statute allows domestic use of intercepted evidence as long as a 'significant' international objective is in view at the intercept's inception" *Ning Wen*, 477 F.3d at 897. Defendant is correct in that the facts before the court in *Ning Wen* did not involve the specific issue currently before this Court. In *Ning Wen*, the defendant argued that evidence obtained under FISA — pursuant to an international investigation

for espionage — could not be used in domestic criminal investigations or prosecutions against him once the international investigation ended. *Id.* at 897. The court affirmed the denial of his motion to suppress, however, because after it conducted its own *in camera*, *ex parte* review of the FISA application affidavits, it found that a significant purpose of the FISA order was to obtain international intelligence. *Id.* The basis behind this denial is relevant to the motions currently before this Court, as it clearly shows that this Court must use the "significant purpose" test in determining the admissibility of the FISA material.

Through the aforementioned *in camera* and *ex parte* review of the FISA electronic surveillance material as it pertains to Defendant, the Court finds that a "significant purpose" of the FISA surveillance was to gather foreign intelligence information. This "measurable foreign intelligence purpose" complies with the requirements of 50 U.S.C. § 1804(a)(7)(B). *Sealed Case*, 310 F.3d at 735.

Defendant argues that because one of the enumerated offenses for which the Government could obtain a Title III electronic surveillance order is providing material support to terrorists, Congress intended that Title III should govern criminal investigations. Defendant does not cite any persuasive authority, however, which holds that Title III precludes the government from seeking to obtain criminal investigation or prosecution evidence

through a FISA order. FISA and Title III can and do co-exist. In addition, several requirements exist to obtain a FISA order that do not exist to obtain a Title III order. These include FISA's requirement that the certification come from an upper-level Executive Branch official, the FISA Court's continuing oversight of the minimization procedures during the surveillance period, and more extensive reporting requirements. *Sealed Case*, 310 F.3d at 740–41. These requirements "bear[] on [FISA's] reasonableness under the Fourth Amendment." *Id*. at 742. Because FISA, both on its face and as applied to Defendant, does not violate the Fourth Amendment, Defendant's Motion to Suppress Electronic Surveillance Evidence Collected Pursuant to FISA is denied.

**C. Request for a *Franks* Hearing**

The Court finally turns to Defendant's Request for a Hearing to Challenge the Veracity of Factual Statements in the Government's FISA Application. In *Franks v. Delaware*, the Supreme Court set forth the now well-established rule that the Fourth Amendment permits criminal defendants to challenge the veracity of affidavits that establish probable cause for a warrant. An electronic surveillance order is characterized as a warrant for purposes of Fourth Amendment review. *See Ning Wen*, 477 F.3d at 897–98. The due process underpinnings of *Franks*, therefore, apply to the government's process of obtaining a FISA order. *See Duggan*, 743 F.2d at 77 n.6. A defendant in a case that involves a FISA order,

however, does not automatically receive a *Franks* hearing. Rather, the FISA order challenger must make "a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included" in the FISA application, as well as establish that the allegedly false statement was "necessary" for the FISC to approve the application. *See Franks*, 438 U.S. at 155–56; *see also Duggan*, 743 F.2d at 77 n.6. Failure to satisfy either of these prongs proves fatal to a *Franks* hearing request. *See Mubayyid*, 521 F.Supp.2d at 130–31.

Defendant has failed to satisfy the requirements to obtain a *Franks* hearing. He has not made any showing — let alone a substantial one — that an Executive Branch officer knowingly and intentionally, or recklessly, included a false statement in the FISA application. Without such a showing, he is foreclosed from obtaining a hearing. Defendant argues that by denying him a *Franks* hearing, the Court gives the FISA evidence "an easier path to admissibility." Under Seal Mem. of Law in Supp. of Def. Rana's Mot. to Suppress Electronic Evidence Collected Pursuant to FISA and Req. for a *Franks* Hr'g 11, Aug. 27, 2010, ECF No. 117. Without producing the requisite offer of proof of impropriety in the FISA application, however, this argument is merely conclusory, and equates to an improper direct attack on the FISA procedures. *See Franks*, 438 U.S. at 171; *see also Damrah*, 412 F.3d at 624–25 ("*Franks* does not apply to a challenge of the underlying procedures

themselves, but rather to the attempt to sidestep the underlying procedures.").

The Court recognizes the frustrating position from which Defendant must argue for a *Franks* hearing. *Franks* provides an important Fourth Amendment safeguard to scrutinize the underlying basis for probable cause in a search warrant. The requirements to obtain a hearing, however, are seemingly unattainable by Defendant. He does not have access to any of the materials concerning the FISA application or surveillance; all he has is notice that the government plans to use this evidence against him.

Nevertheless, to challenge the veracity of the FISA application, Defendant must offer substantial proof that the FISC relied on an intentional or reckless misrepresentation by the government to grant the FISA order. The quest to satisfy the *Franks* requirements might feel like a wild-goose chase, as Defendant lacks access to the materials that would provide this proof. This perceived practical impossibility to obtain a hearing, however, does not constitute a legal impossibility. If Defendant obtains substantial proof that the FISC relied upon an intentional or recklessly false statement to approve the FISA order, he could obtain a hearing. In addition, the Court has already undertaken a process akin to a *Franks* hearing through its *ex parte*, *in camera* review of the FISA materials. 50 U.S.C. § 1806(f). Through this

review, the Court finds that Defendant is not entitled to a *Franks* hearing. Therefore, his request is denied.

## IV. CONCLUSION

For the reasons stated herein, the Court rules as follows:

1. Defendant's Motion to Disclose FISA Applications, Orders, and Related Documents is denied.

2. Defendant's Motion to Suppress Electronic Surveillance Evidence Collected Pursuant to FISA is denied.

3. Defendant's Request for a *Franks* Hearing is denied.

**IT IS SO ORDERED.**

Harry D. Leinenweber, Judge
United States District Court

**DATE:** 11/10/2010