IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF OREGON

EUGENE DIVISION

| | | |
|---|---|---|
| UNITED STATES OF AMERICA, | ) | Cr. No. 05-60008-HO |
| | ) | |
| Plaintiff, | ) | ORDER |
| | ) | |
| v. | ) | |
| | ) | |
| PIROUZ SEDAGHATY, et al., | ) | |
| | ) | |
| Defendants. | ) | |
| | ) | |

On February 13, 2004, Colleen Anderson, a special agent with the Internal Revenue Service's Criminal Investigation Division, submitted an affidavit seeking a search warrant for the premises at 3800 S. Highway 99 in Ashland, Oregon owned by Al Haramain Islamic Foundation, Inc. (Al Haramain USA).[1] Magistrate Judge Cooney approved the application and issued the warrant to search for evidence related to subscription to a false tax form 990 violation

[1]The listing of items to be seized did list several Al Haramain associated organizations, including Al Haramain Riyadh.

for the year 2000 and evidence related to a failure to file a currency and monetary instrument report violation including bank records, transaction records, and including such information on computers. The list of items to be seized included a protocol for searching computers and what to do with items on computers not within the scope of the warrant.

Prior to the search, a review with the search officers was conducted regarding the protocol, screening, what to do with possible attorney/client privilege items, etc. The search was conducted on February 18, 2004, and among the items seized were nine computers and assorted computer media. When agents arrived, defendant's son Jonah Sedaghaty and his girlfriend were present. Jonah called an attorney, David Berger, who stated that he was a family attorney and an attorney for Al Haramain. Berger reviewed the warrant and affidavit. Berger and Jonah gave consent to search containers not listed in the warrant. Jonah and Berger also gave consent to seize items not listed in the warrant including video tapes, boxes of correspondence, photos, samples of literature, noble Korans, etc. Berger reviewed the evidence seized before it was taken from the search location.

A computer specialist later imaged all nine of the computers' hard drives and the computers were returned to Berger within 60 days after execution of the warrant. The computer related items were retained for analysis. The computer hard drives had been

deleted and analysts were able to access some data after a lengthy process. Analysis of the drives sometimes revealed items unrelated to the warrant and FBI agent Timothy Suttles applied for a new warrant for some of the materials. Review of the seized evidence was somewhat dormant during the time defendant Pirouz Sedaghaty and defendant Al Buthe were out of the United States. When Sedaghaty returned, the investigation intensified.

The affidavit in support of the warrant related the following:

Defendant Sedaghaty purchased the property searched on behalf of Al Haramain with $190,000 in funds brought to him from Saudi Arabia by Al Buthe. Sedaghaty lived at the property and used it as a prayer house and to conduct Al Haramain business.

In 1999, Sedaghaty incorporated Al Haramain Islamic Foundation in Oregon and filed an application to become a tax exempt organization.

Egyptian Mahmoud Talaat El-Fiki made a $150,000 donation to Al Haramain Islamic Foundation in February of 2000 in order to participate in support of "our Muslim brothers in Chychnya." The general manager of Al Haramain in Saudi Arabia was Aqeel Abdul-Aziz Al-Aqeel who was also the President of Al Haramain in Oregon. Al-Aqeel thanked El-Fiki for the donation, assuring him of every possible effort to help ending the Chechnyan crisis. El-Fiki wired the money from Kuwait to an Ashland, Oregon Bank of America branch.

On March 7, 2000, Al Buthe flew from Saudi Arabia to Oregon. On March 10, 2000, Al Buthe, defendant Sedaghaty and Sedaghaty's son went to the Bank Of America in Ashland and Al Buthe purchased 130 $1,000 travelers checks using the El Fiki donation. The next day, Sedaghaty purchased a $21,000 cashier's check, using the remaining donation funds, made payable to Al Buthe. On the front of the check someone wrote donation for Chechnya refugees. Records obtained from Al Haramain Islamic Foundation showed that Sedaghaty and Al Buthe signed an agreement on March 11, 2000 stating that Sedaghaty was turning over the funds to Al Buthe for the "Brothers and Sisters in Chechnya."

Al Buthe returned to Saudi Arabia on March 12, 2000. Federal law requires anyone transporting currency in any form over $10,000 in or out of the U.S. to submit a currency monetary instrument report (CMIR). Al Buthe did not file the CMIR when he left the United States. Al Buthe did file CMIRs on nine separate prior occasions and is proficient in reading and writing English.

Al Buthe cashed the 130 $1,000 traveler's checks on about March 25, 2000, at a bank in Riyadh and deposited the $21,000 cashier's check.

To account for the El Fiki donation, Sedaghaty hired accountant Thomas Wilcox to prepare a form 990. Sedaghaty provided Wilcox with computerized accounting records depicting the El Fiki donation as being used to purchase a prayer house in Springfield,

Missouri, and indicated that some of the funds were returned to El Fiki. Sedaghaty did not provide any information to Wilcox indicating the funds had gone to Chechnya or any bank records or receipts Sedaghaty and Al Buthe signed for the funds. Agent Anderson showed Wilcox the records who then acknowledged that the Form 990 contained false information.

The affidavit also detailed the connection between the El Fiki funds and Chechnya and also detailed the Chechnyan mujahideen and Islamic charities. The affidavit related that information had been obtained from an international terrorism consultant. The affidavit also included newspaper and periodical reports about the Chechnyan resistance evolving into an attempt to create an Islamic state and that Al Haramain was suspected of providing weapons.

The affidavit further related that the Office of Foreign Asset Control (OFAC) designated several Al Haramain offices as supporters of terrorism. The affidavit also detailed why Anderson believed information regarding the failure to report and tax fraud would be at the Ashland residence, despite defendant Sedaghaty's absence, including Al Haramain banking activity still being conducted and that, in January 2003, records and computers were located there.

As noted above, the search resulted in many items and media being seized and the government retaining hard drive images for continued analysis. Defendant moves to suppress evidence seized

pursuant to the warrant and to compel the government to cease all searches of the computers and electronic media seized.

A. Prior Unlawful Activity

Defendant first asserts that illegal activity on the part of the government tainted the search by speculating that the Terrorist Surveillance Program (TSP) resulted in incorporation of the fruits of an alleged illegal search/surveillance application or that the decision to seek the warrant was based on the alleged illegal search/surveillance. Prior unlawfully obtained evidence will not serve to invalidate a search pursuant to a warrant if the search pursuant to the warrant was in fact motivated by a genuinely independent source. In this case, if the agents' decision to seek the warrant was not prompted by what they had seen during any unlawful activity, and information resulting from the purported illegal activity is not presented to the Magistrate affecting his decision to issue the warrant, then the warrant is valid. See, Murray v. United States, 487 U.S. 533, 542 (1988).

Defendant relies on public information regarding litigation involving Al Haramain and publically available information regarding the TSP along with information regarding the length of the investigation, involvement of several government agencies, the efforts to designate Al Haramain and the designation, and speculation. There is no reason to believe the activity on the

part of the government regarding possible warrantless surveillance, to the extent such activity exists and was illegal, resulted in any information being used in the affidavit in support of the search warrant or prompted the decision to seek the warrant. The motion to suppress is denied on this basis.

Special Agent Colleen Anderson had no knowledge of any illegal surveillance program or even knowledge about what is publically known of the TSP. Moreover, it appears that intercepts did not involve defendant Sedaghaty, but co-defendant Al Buthe and lawyers in D.C., according to defendant. Anderson also states that she did consult with OFAC (the agency making the designation) regarding the logistics of the search and did not obtain any information from OFAC to use in her affidavit.

Defendant also contends that there is further evidence of unlawful surveillance of him and AL Haramain. Specifically, defendant cites video surveillance and "weathering" on wiring near the residence and speculates, based on conclusions offered by Colonel Walter Lang (retired), that government agents in D.C. and not Medford made the decision to seek the warrant at issue based on illegal surveillance.

The court has already ruled on many CIPA issues in this area after reviewing documents and finding them to be of no exculpatory value in this regard. Defendant's speculation as to illegal

surveillance does not warrant suppression of the items seized pursuant to the search warrant.

B. Seizure Exceeded the Scope of the Warrant

Defendant next argues that all fruits of the search must be suppressed, because the executing agents exceeded the scope and protocols of the warrant, relying on the Tenth Circuit's admonition that "[w]hen law enforcement officers grossly exceed the scope of a search warrant in seizing property, the particularity requirement is undermined and a valid warrant is transformed into a general warrant thereby requiring suppression of all evidence seized under that warrant." United States v. Medlin, 842 F.2d 1194, 1199 (10th Cir. 1988).

As explained by the Ninth Circuit:

> It is highly doubtful whether the wholesale seizure by the Government of documents not mentioned in the warrant comported with the requirements of the fourth amendment. As a general rule, in searches made pursuant to warrants, only the specifically enumerated items may be seized.... It is true that all items in a set of files may be inspected during a search, provided that sufficiently specific guidelines for identifying the documents sought are provided in the search warrant and are followed by the officers conducting the search.... However, the wholesale seizure for later detailed examination of records not described in a warrant is significantly more intrusive, and has been characterized as "the kind of investigatory dragnet that the fourth amendment was designed to prevent."...
>
> In the comparatively rare instances where documents are so intermingled that they cannot feasibly be sorted on site, we suggest that the Government and law enforcement officials generally can avoid violating fourth amendment

> rights by sealing and holding the documents pending approval by a magistrate of a further search .... If the need for transporting the documents is known to the officers prior to the search, they may apply for specific authorization for large-scale removal of material, which should be granted by the magistrate issuing the warrant only where on-site sorting is infeasible and no other practical alternative exists.

United States v. Tamura, 694 F.2d 591, 595-596 (9th Cir. 1982).

Defendant attacks the seizure of the computers and related media and argues that the agents generally rummaged though e-mail accounts or miscellaneous saved files including personal e-mails, attorney-client e-mails, photographs, news articles, web pages, internal organization documents, private family communications, and vacation plans well beyond the confines of the items described in and the protocols established by the warrant.

Defendant asks that, at a minimum, the materials seized outside the warrant be suppressed, if not all of the evidence.

However, the warrant permitted seizures of the computers and media. Agent Anderson described a careful search protocol in which a search of the computers and data was done with search terms carefully tailored to information related to the items to be seized listed in the warrant. A taint team was utilized and coordination with the AUSA implemented whenever questions regarding whether information was covered by the warrant. The affidavit adequately explained why the computers had to be taken off-site for review and why they would likely contain evidence within the scope of the affidavit. Given the nature of the data and the fact that it had

been deleted, the actions taken by the government were reasonable and permitted by the warrant as approved by Magistrate Cooney. See U.S. v. Banks, 556 F.3d 967, 973-74 (9th Cir. 2009) (A generalized seizure of business documents may be justified if it is demonstrated that the government could not reasonably segregate documents on the basis of whether or not they were likely to evidence criminal activity). See also, United States v. SDI Future Health Inc., 568 F.3d 684, 699 9th Cir. 2009) (an affidavit is part of a warrant, and therefore potentially curative of any defects, if (1) the warrant expressly incorporated the affidavit by reference and (2) the affidavit either is attached physically to the warrant or at least accompanies the warrant while agents execute the search).

The crimes charged require proof of intent and thus records beyond simple financial records were appropriately seized, such as evidence of support of the efforts of the Chechnyan mujahideen. Moreover, search terms were used to limit the search of the computer files to find items reasonably related to the items described in the warrant and affidavit. The fact that a further warrant was requested when information possibly relating to a separate crime was discovered belies the allegations that the search was a general fishing expedition.

In short, the warrant, including the affidavit incorporated into the warrant, was reasonably specific as to the items sought

and the government followed appropriate protocols to separate intermingled materials. The care used in this case appears to actually exceed what is required given the nature of white collar crimes and the intermingling of information on computers. This is especially true in light of the use of carefully tailored search terms.

Defendant also contends that suppression should be ordered because the government has continued to search the retained images of the computers and media. However, defendant appears to confuse the propriety of an endless search with retention and analysis of appropriately seized materials. The computers and media have been returned and the government merely continues to analyze the material copied. The delay in analysis is also related to defendant's fugitive status for such a long period of time. The seizure was appropriate and thus retention is not a basis for suppression.

Defendant brings to the court's attention the *en banc* decision in United States v. Comprehensive Drug Testing, Inc., 579 F.3d 989 (9th Cir. 2009). Defendant contends the case buttresses his argument that the government exceeded the scope of the warrant when it searched the computer hard drives. Specifically, defendant notes that

> In Comprehensive Drug Testing, Inc. (CDI), the en banc court strongly confirmed the importance of the procedures set forth in United States v. Tamura, 694 F.2d 591 (9th Cir. 1982) to computer searches, stating that the point

> of the procedures is to "maintain the privacy of materials that are intermingled with seizable materials, and to avoid turning a limited search for particular information into a general search of office file systems and computer databases." CDI, No. 05-10067 at 11876. This limitation prevents the government from conducting a general search under the pretense of looking for information that falls within the scope of the warrant and coming upon other information, claiming it was in "plain view." Id. at 11877. The data on computers must first be segregated and this must be done by specialized personnel or a third party. Id. at 11892. Once data has been properly segregated, "the government agents involved in the investigation may examine only the information covered by the terms of the warrant." Id. at 11881. In CDI, the Court also held that, absent further judicial authorization, any other copies must be destroyed or returned along with the actual physical medium seized, to the party from whom they were seized. Id. "Also, within a time specified in the warrant, which should be as soon as practicable, the government must provide the issuing officer with a return disclosing precisely what data it has obtained as a consequence of the search, and what data it has returned to the party from whom it was seized." Id.

Supplement to Defendant's Motion to Suppress (#213) at pp. 2-3.

It should be noted that the Ninth Circuit did not intend the rules it prescribed in Comprehensive Drug Testing be applied retroactively. See United States v. Wilbur, 2010 WL 519735 (W.D.Wash. Feb 4, 2010).[2] The warrant and seizure in this case predates the case. Nonetheless, defendant cites the case to show confirmation of the long-standing rule of Tamura. As noted, the search in this case did not amount to a general fishing expedition.

---

[2]Comprehensive Drug Testing set out a host of new procedures to be utilized in writing search warrants and subsequently searching contents of electronic evidence, dramatically altering the manner in which the government will be able to obtain future warrants and search electronically stored information seized pursuant to such warrants.

Agent Anderson testified as to the procedures used by the government in seeking the warrant, the terms of the warrant and the conduct of the executing and reviewing officers. Ninth Circuit case law prior to Comprehensive Drug Testing allowed the search procedure utilized here.

> Although computer technology may in theory justify blanket seizures ... the government must still demonstrate to the magistrate factually why such a broad search and seizure authority is reasonable in the case at hand. There may well be situations where the government has no basis for believing that a computer search would involve the kind of technological problems that would make an immediate onsite search and selective removal of relevant evidence impracticable. Thus, there must be some threshold showing before the government may "seize the haystack to look for the needle."

United States v. Hill, 459 F.3d 966, 975 (9th Cir. 2006). There have been cases in which the Ninth Circuit has allowed removal of electronic media for off-site analysis. See, e.g., United States v. Hay, 231 F.3d 630, 637 (9th Cir. 2000) (allowed generic classification authorizing seizure of an entire computer system and virtually every document in the defendant's possession without referencing child pornography or any particular offense conduct because, although officers knew that a party had sent 19 images of child pornography directly to the defendant's computer, they had no way of knowing where the images were stored.); United States v. Lacy, 119 F.3d 742, 746 (9th Cir. 1997) (no more specific description of the computer equipment sought was possible, because

the agents did not know whether the images were stored on the hard drive or on one or more of the defendant's many computer disks).

As noted above, the circumstances of this case justified the extensive search of the hard drives (limited by search terms and circumscribed by a taint team) for the materials permitted to be seized by the warrant because the materials such as financial documents and documents related to intent could be stored anywhere on the hard drives and were in a form (deleted) that necessitated extensive off-site review that was limited by appropriate protocols. Defendant argues that during the hearing, government counsel seemingly admitted unlimited searches. This contention is refuted by the record support of the protocols.

In his second supplement, defendant revisits the computer search as beyond the scope of the warrant, arguing that there were substantive unguided reviews of the hard drives for five months. Defendant also contends that Agent Anderson's testimony regarding when she became involved in the investigation is inconsistent with discovery provided.

Defendant maintains that a report from FBI agent Richard Smith reveals extensive review of the hard drives conducted by the FBI and that the review involved searches for evidence not contained within the warrant. Defendant also pieces together various discovery and asserts that it appears that searches were conducted in 2004, but that search terms were not developed until 2008.

It appears that what happened in 2004 was a process to reconstruct the corrupted or deleted data on the hard drives and then once reconstructed, to use search terms to look for evidence within the scope of the warrant. This was an appropriate search.

Defendant also contends that Agent Anderson offered testimony inaccurately portraying the time period in which she became involved with the investigation (2002), based on documents stamped received by Anderson in 2001. However, the file stamps show nothing more than receipt by the FBI generally and not IRS agent Anderson specifically. The court finds that Agent Anderson did not testify falsely in this regard.

C. Probable Cause

Defendant next contends that the warrant lacked probable cause and was infected by material misstatements and omissions and was so defective in this regard that the good faith exception does not apply. The court conducted a hearing on this issue.

Probable cause is a flexible, common-sense standard. It merely requires that the facts available to the officer would lead a man of reasonable caution to believe that certain items may be contraband or stolen property or useful as evidence of a crime; it does not demand any showing that such a belief be correct or more likely true than false. Texas v. Brown, 460 U.S. 730, 742 (1983).

A determination of probable cause depends on the totality of the circumstances. Illinois v Gates, 462 U.S. 213, 238 (1983).

A magistrate's determination of probable cause to issue a search warrant is accorded great deference and is reversed only if that determination is clearly erroneous. United States v. Espinosa, 827 F.2d 604, 610 (9th Cir. 1987). "[T]he traditional standard for review of an issuing magistrate's probable cause determination has been that so long as the magistrate had a 'substantial basis for ... conclud[ing]' that a search would uncover evidence of wrongdoing, the Fourth Amendment requires no more." Illinois v. Gates, 462 U.S. 213, 236 (1982) (quoting Jones v. United States, 362 U.S. 257, 271 (1960)). "In borderline cases, preference will be accorded to warrants and to the decision of the magistrate issuing it." United States v. Martinez, 588 F.2d 1227, 1234 (9th Cir. 1987).

A magistrate is permitted to draw reasonable inferences about where evidence is likely to be kept based on the nature of the evidence and the type of offense. United States v. Angulo-Lopez, 791 F.2d 1394, 1399 (9th Cir. 1986). He need not determine that the evidence sought is in fact on the premises to be searched or that the evidence is more likely than not to be found where the search takes place. The magistrate need only conclude that it would be reasonable to seek the evidence in the place indicated in the affidavit. United States v. Peacock, 761 F.2d 1313, 1315 (9th Cir.

1985). Moreover, "a magistrate may rely on the conclusions of experienced law enforcement officers regarding where evidence of a crime is likely to be found." United States v. Fannin, 817 F.2d 1379, 1382 (9th Cir. 1987).

Defendant argues that the entire premise of the alleged wrongdoing in the warrant application is the desire to fund the Chechnyan mujahideen, but that the warrant application merely offers newspaper accounts which are unreliable. The affidavit in support of the warrant, however, provided more than newspaper accounts, including information provided by an international terrorism expert and the designation of several other Al Haramain branches. The motion to suppress is denied on this basis.

The defense next takes issue with alleged material misstatements and omissions in the warrant application. In Franks v. Delaware, 438 U.S. 154, 98 S.Ct. 2674, 57 L.Ed.2d 667 (1978), the Supreme Court held that in order to challenge an affidavit valid on its face, a defendant must show (1) the affidavit contains intentionally or recklessly false statements, and (2) the affidavit purged of its falsities would not be sufficient to support a finding of probable cause. The Court in Franks placed special emphasis on the strict requirement of proof, finding that "[t]here must be allegations of deliberate falsehood or of reckless disregard for the truth, and those allegations must be accompanied by an offer of proof." Id. at 171.

To show entitlement to a Franks hearing, the defendant must make specific allegations that indicate the portions of the warrant claimed to be false. Id. There must be a contention of deliberate falsehood or reckless disregard for the truth. Id. The allegations must be accompanied by a detailed offer of proof, preferably in the form of affidavits. The offer of proof must challenge the veracity of the affiant, not that of his informant. Id. Finally, the challenged statements in the affidavit must be necessary to a finding of probable cause. United States v. Flores, 679 F.2d 173, 176 (9th Cir. 1982).

Many of the alleged misstatements are innocuous, such as the claim that the requesting agent failed to note that travelers checks are used in the normal course of business.

Defendant argues that Al Haramain Islamic Foundation and Al Haramain USA are portrayed as the same organization and that the affidavit fails to state that an investigation began a few years prior to the search request. There is, of course, a strong connection between Al Haramain Riyadh and Al Haramain USA, especially since the general manager in Riyadh was also the president of Al Haramain USA at the time and Al Buthe moved money on behalf of Al Haramain Riyadh. The investigation of Al Haramain prior to the search warrant application does not impact the finding of probable cause.

The omissions regarding a different view of the Chechnyan conflict is immaterial because the information was offered to show false reporting, not a political point. Also, Anderson's assertion that other similar transactions to the Chechnya transactions may be found, even if unsupported, does not destroy probable cause.

The failure to include Wilcox's statement that he never thought Sedaghaty was intentionally dishonest is not material as the affidavit related that Sedaghaty told Wilcox the forms had to be right and clean and the statement preceded Wilcox being shown the various falsities in the form 990.

Defendant contends the affidavit should have related that Wilcox was more than a tax preparer, but the affidavit also noted that Wilcox provided some training in Quickbooks and the omission that Wilcox once worked for the IRS is not material.

The lack of information regarding the length of the investigation in paragraph 66, and how Anderson came to know there did not appear to be any religious activity at the address and that Jonah Sedaghaty lived there is not material.

The information regarding the FBI contacts in 2001 is not pertinent.

Defendant raises several other alleged omissions regarding the peaceful nature of Sedaghaty and cooperation with the FBI by providing an e-mail account, but this does not affect the probable

cause finding. Moreover, much of the information regarding peaceful activity resulted from the search itself.

Defendant also takes issue with the consent provide by Jonah Sedaghaty. The consent argument is largely based on the alleged invalidity if the warrant as opposed to voluntariness in terms of coercion.

There are five main factors to assess the voluntariness of consent:

> (1) whether defendant was in custody; (2) whether the arresting officers had their guns drawn; (3) whether Miranda warnings were given; (4) whether defendant was notified that he had a right not to consent; and (5) whether the defendant has been told a search warrant could be obtained.

United States v. Soriano, 346 F.3d 963, 968-969 (9th Cir. 2003). No one factor is dispositive in determining consent. United States v. Chan-Jimenez, 125 F.3d 1324, 1327 n.3 (9th Cir. 1997). There appears to be no issue with respect to these factors and there appears to be no issue regarding authority to consent either. As noted above, the warrant was valid.

The motion to suppress is denied. There is an insufficient showing regarding whether any illegal government activity played a role in the decision to seek a search warrant or provided support for probable cause in the affidavit. The motion to compel the government to cease all searches of the imaged hard drives and other computer media is also denied. And, in this regard, the

government's request to resume analysis of the computer media is granted.

In "motion" number 205, defendant asserts that Agent David Carroll testified that the hard drives were provided to the Russian FSB (Federal'naya Sluzhba Bezopasnosti (Federal Security Service)), and defendant believes such provision was part of a *quid pro quo* arrangement. Defendant argues that the provision of the hard drives to the Russian government constitutes such outrageous conduct that suppression of the evidence obtained from the drives is required. The government responds that both the United States and the Russian Federation have an interest in preventing the financing of terrorist activity and in stopping the provision of material support to terrorist organizations in all parts of the world, including in that part of the Russian Federation called Chechnya. Indeed, suicide bombers recently killed eight policeman in two incidents in Chechnya and an Islamic terrorist group claimed responsibility for one of the attacks.[3]

In a joint effort to fight terrorism, the United States and the Russian Federation exchange information and evidence concerning the activities of Al Haramain. The information exchange at issue apparently took place in 2008.

---

[3]As late as Monday, March 29, 2010, suicide bombers believed to be connected to the rebels from the restive Caucasus region that includes Chechnya, killed at least 38 in Moscow's subway.

The two countries are parties to a treaty requiring exchange of information.[4] At a December 2008 meeting, representatives of the Russian FSB provided the United States with certain evidence relevant to this prosecution, as requested by the United States under the Treaty. For example, the Russian FSB disclosed that it had learned that Al Haramain had smuggled money into Chechnya through an Al Haramain office in Baku, Azerbaijan. Some of this money was funneled to the Kavkaz Islamic Institute, which was a training camp for the mujahideen in Chechnya. The money from this so-called charity was used "to purchase weapons, uniforms, medicine, communication devices, vehicles, and to pay religious extremists' salaries."

Similarly, according to the FSB, the Russian government intercepted a message from Aqeel Aqeel, who was both the head of Al Haramain in Saudi Arabia as well as the President of Al Haramain USA in Ashland, Oregon, to Ibn Khattab, a Saudi citizen who was the head of the foreign mujahideen fighting the Russians in Chechnya. The message contained information regarding a weapons shipment.

At this December 2008 meeting, U.S. law enforcement provided a copy of the computer hard drives seized from Al Haramain USA in

---

[4]Most recently, Presidents Obama and Medvedev continued implementation of this arrangement by creating a Bilateral Presidential Commission with several working groups, including a "Foreign Policy and Fighting Terrorism Group" chaired by the U.S. Undersecretary of State and the Russian Deputy Foreign Minister. Fact Sheet: U.S.-Russia Bilateral Presidential Commission, released by the Office of the Press Secretary, The White House, July 6, 2009.

Oregon pursuant to the warrant. Those hard drives contained substantial evidence of interest to the Russian government in its on-going efforts to counter terrorism in the Caucasus. For example, the Al Haramain USA hard drives contained the photographs of captured and dead Russian soldiers, as well as photographs of some of their identity papers. It is understandable that Russia might have an interest in examining the Al Haramain USA computers to account for its own soldiers. Other information relevant to jihads in Chechnya from the computers were provided.

The Foreign Intelligence Surveillance Act (FISA) provides for the sharing of information to protect against attacks. 50 U.S.C. § 403-5d(1). The information shared in this case falls within the Act, despite its age. Such conduct does not approach a level of outrageousness sufficient to justify exclusion of lawfully seized evidence. The fact that the drives may hold other information potentially outside the information allowed to be shared under FISA does not change such a finding given the difficult nature of retrieving the information and the possibility that other relevant information may be discovered by Russian forensics. The tools at the disposal of the Russians may very well uncover deeper information related to terrorist activity than U.S. forensics and, thus, it was arguably necessary to provide the entire images and not outrageous. Moreover, there is no evidence of the Russians providing information obtained from the drives which demonstrate an

illegal search or illegally obtaining information beyond the scope of the warrant on the part of the United States government.

To the extent document number 205 is a motion to suppress, the motion is denied.

## CONCLUSION

For the reasons stated above, defendant's motions to suppress (#s 181, 205) and defendant's motion to stop all searches of computers and electronic media seized on February 18, 2004 (#182) are denied.

DATED this 13th day of April, 2010.

s/ Michael R. Hogan
United States District Judge