Jon B. Eisenberg, California Bar No. 88278 (jon@eandhlaw.com)
William N. Hancock, California Bar No. 104501 (bill@eandhlaw.com)
Eisenberg & Hancock LLP
1970 Broadway, Suite 1200 • Oakland, CA 94612
510.452.2581 – Fax 510.452.3277

Steven Goldberg, Oregon Bar No. 75134 (steven@stevengoldberglaw.com)
River Park Center, Suite 300 • 205 SE Spokane St.• Portland, OR 97202
503.445-4622 – Fax 503.238.7501

Thomas H. Nelson, Oregon Bar No. 78315 (nelson@thnelson.com)
P.O. Box 1211, 24525 E. Welches Road • Welches, OR 97067
503.622.3123 - Fax: 503.622.1438

Zaha S. Hassan, California Bar No. 184696 (zahahassan@comcast.net)
8101 N.E. Parkway Drive, Suite F-2.• Vancouver, WA 98662
360.213.9737 - Fax 866.399.5575

J. Ashlee Albies, Oregon Bar No. 05184 (ashlee@sstcr.com)
Steenson, Schumann, Tewksbury, Creighton and Rose, PC
815 S.W. Second Ave., Suite 500 • Portland, OR 97204
503.221.1792 – Fax 503.223.1516

Lisa R. Jaskol, California Bar No. 138769 (ljaskol@earthlink.net)
610 S. Ardmore Ave.• Los Angeles, CA 90005
213.385.2977 – Fax 213.385.9089

Attorneys for Plaintiffs Al-Haramain Islamic Foundation, Inc., Wendell Belew and Asim Ghafoor

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

IN RE NATIONAL SECURITY AGENCY TELECOMMUNICATIONS RECORDS LITIGATION	MDL Docket No. 06-1791 VRW
This Document Relates Solely To:	**MOTION PURSUANT TO 50 U.S.C. § 1806(f) TO DISCOVER OR OBTAIN MATERIAL RELATING TO ELECTRONIC SURVEILLANCE**
Al-Haramain Islamic Foundation, Inc., et al. v. Bush, et al. (C07-CV-0109-VRW)	Date: Tuesday, December 2, 2008 Time: 10:00 a.m.
AL-HARAMAIN ISLAMIC FOUNDATION, INC., et al.,	Court: Courtroom 6, 17th Floor Honorable Vaughn R. Walker

Plaintiffs,

vs.

GEORGE W. BUSH, President of the United States, et al.,

Defendants.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page

CASES

STATUTES

MISCELLANEOUS

NOTICE OF MOTION

TO ALL PARTIES AND THEIR COUNSEL OF RECORD:

PLEASE TAKE NOTICE that on Tuesday, December 2, 2008, at 10:00 a.m., before the Honorable Vaughn R. Walker, United States District Chief Judge, in Courtroom 6, 17th Floor, 450 Golden Gate Avenue, San Francisco, California, the plaintiffs in *Al-Haramain Islamic Foundation, Inc. v. Bush* (07-CV-109-VRW) will move and hereby do move the Court, pursuant to 50 US.C. section 1806(f), for an order allowing plaintiffs to discover or obtain material relating to electronic surveillance.

By this motion, plaintiffs seek access, under appropriate security procedures and protective orders as prescribed by section 1806(f), to portions of the Sealed Document filed with the Court at the outset of this litigation on February 28, 2006.

* * * * *

MEMORANDUM OF POINTS AND AUTHORITIES

INTRODUCTION

This motion under 50 U.S.C. section 1806(f) seeks access to the Sealed Document plaintiffs filed on February 28, 2006, for the limited purpose of including portions of the Sealed Document as part of plaintiffs' showing of their standing to prosecute this action to determine whether the President has power to disregard the Foreign Intelligence Surveillance Act (FISA).

Plaintiffs have filed an amended complaint which presents abundant unclassified information demonstrating plaintiffs' electronic surveillance in March and April of 2004. In this memorandum of points and authorities, we demonstrate how the amended complaint shows plaintiffs' status as "aggrieved persons" – meaning that they were subjected to "surveillance" and that their surveillance was "electronic"– which gives this Court discretion to afford plaintiffs access to the Sealed Document "under appropriate security procedures and protective orders." 50 U.S.C. § 1806(f). We show that plaintiffs' burden of proving their "aggrieved person" status is to produce unclassified prima facie evidence, direct and/or circumstantial, sufficient to raise a reasonable inference on a preponderance of the evidence that they were subjected to electronic surveillance. We further show how plaintiffs have met this burden with the unclassified information set forth in the amended complaint, which

includes the FBI's admission that defendants surveilled plaintiffs, a wealth of direct and circumstantial evidence raising a compelling inference that the admitted surveillance included international telecommunications by plaintiffs Wendell Belew and Asim Ghafoor in March and April of 2004, and evidence demonstrating the probability that defendants' interception of those telecommunications was electronic within the meaning of FISA. Finally, we propose several possible security measures by which plaintiffs can safely be given access to portions of the Sealed Document without endangering national security.

STATEMENT OF ISSUES TO BE DECIDED

1. What facts must plaintiffs show to establish that they are "aggrieved persons" who may discover or obtain material relating to electronic surveillance under section 1806(f)?

2. What is the appropriate standard of proof for determining whether plaintiffs have demonstrated "aggrieved person" status under section 1806(f)?

3. Does the unclassified evidence presented in plaintiffs' amended complaint meet the standard of proof under section 1806(f)?

4. What security measures can be imposed that would safeguard plaintiffs' access to the Sealed Document that is the subject of this motion?

STATEMENT OF RELEVANT FACTS

A. Public admissions that defendants conducted warrantless electronic surveillance.

Shortly after the terrorist attacks of September 11, 2001, defendants commenced a program of warrantless electronic surveillance of international telecommunications, intercepting them domestically from routing stations located within the United States. Defendants Bush and Alexander, former Attorney General Alberto Gonzales, former Deputy Assistant Attorney General John Yoo, and the Department of Justice (DOJ) have each made public statements admitting that, under the program, the President authorized the National Security Agency (NSA) to intercept, without court orders, international communications into and out of the United States of persons believed to be "a member," "affiliated with," "linked to," "a member of an organization affiliated with," or "working in support of" al-Qaeda. *See* Decl. of Jon B. Eisenberg, exhs. A at 3, B at 6, C at 8, D at 11, E at 13, F at 16.

//

B. Public evidence that defendants knew the warrantless surveillance program was unlawful yet continued it for several weeks in 2004 without DOJ certification.

On May 15, 2007, in testimony before the Senate Judiciary Committee, and on May 22, 2007, in written answers to follow-up questions by Senator Patrick Leahy, former Deputy Attorney General James B. Comey made the following statements demonstrating that defendants knew the warrantless surveillance program was unlawful yet continued it for several weeks in 2004 without the DOJ's approval:

- As of early March of 2004, Comey and Attorney General John Ashcroft had determined that the program was unlawful. *See id.*, exh. G at 20-21, 29.
- During a meeting at the White House on March 9, 2004, two days before the DOJ's periodic written certification of the program was due, Comey told Vice-President Dick Cheney and members of his and defendant Bush's staffs that the DOJ had concluded that the program was unlawful and that the DOJ would not re-certify it. *See id.*, exhs. G at 20-21, 26, 28-29, H at 33, 35.
- On March 10, 2004, while Ashcroft was hospitalized, two White House officials went to Ashcroft's bedside and attempted to obtain the written certification from Ashcroft, but he refused. *See id.*, exh. G at 19, 23.
- Despite the advice that the program as then constituted was unlawful, defendant Bush did not direct Comey or the FBI to discontinue or suspend any portion of the program. *See id.*, exh. G at 24-25, 27, 30.
- On March 11, 2004, the DOJ's certification of the program lapsed without the DOJ's re-certification. *See id.*, exh. G at 27, 30.
- The program continued to operate without the DOJ's certification for a period of several weeks following March 11, 2004. *See id.*, exhs. G at 27-28, 30, H at 35.

On July 26, 2007, defendant Mueller testified before the House Judiciary Committee that prior to the incident at Ashcroft's bedside, Mueller had "serious reservations about the warrantless wiretapping program," and that at or near the time of the incident, during conversations between Comey and defendant Mueller, Comey "expressed concern about the legality of it." *See id.*, exh. I at 39, 40.

C. Public evidence that in February 2004 defendants began investigating Al-Haramain for possible crimes relating to currency reporting and tax laws.

On March 4, 2004, FBI Counterterrorism Division Acting Assistant Director Gary M. Bald testified before the Senate Caucus on International Narcotics Control that in February 2004 defendants began investigating plaintiff Al-Haramain for possible terrorist financing, saying the following:

- The FBI's Terrorist Financing Operations Section (TFOS) participates in joint operations with the Treasury Department to investigate potential terrorist-related financial transactions. *See id.*, exh. J at 43, 45-46.
- The TFOS investigated Al-Haramain "pertaining to terrorist financing." *See id.*, exh. J at 46, 48.
- In February of 2004, the FBI executed a search warrant on Al-Haramain's office in Ashland, Oregon. *See id.*, exh. J at 48.
- The TFOS provided operational support, including document and data analysis, in a subsequent investigation of Al-Haramain. *See id.*, exh. J at 48.

In a press release issued on February 19, 2004, the Treasury Department announced that OFAC had blocked Al-Haramain's assets pending an investigation of possible crimes relating to currency reporting and tax laws. *See id.*, exh. K at 54.

D. Public evidence that the FBI regularly used classified information produced by the warrantless surveillance program.

On September 25, 2003, FBI Deputy Director (at that time Counterterrorism Division Assistant Director) John S. Pistole testified before the Senate Committee on Banking, Housing and Urban Affairs that the TFOS "has access to data and information" from "the Intelligence Community." *See id.*, exh. L at 59. On June 16, 2004, OFAC Director R. Richard Newcomb testified before the House Financial Services Subcommittee on Oversight and Investigations that in conducting investigations of terrorist financing, OFAC officers use "classified . . . information sources." *See id.*, exh. M at 68. On July 26, 2007, defendant Mueller testified before the House Judiciary Committee that in 2004 the FBI, under his direction, undertook activity using information produced by the NSA through the warrantless surveillance program. *See id.*, exh. I at 40, 41.

//

E. The telephone conversations where plaintiffs discussed Ghafoor's representation of persons linked with Osama bin-Laden.

During the period immediately following the blocking of Al-Haramain's assets on February 19, 2004, plaintiff Belew spoke over the telephone with one of Al-Haramain's directors, Soliman al-Buthi, on the following dates: March 10, 11 and 25, April 16, May 13, 22 and 26, and June 1, 2 and 10, 2004. *See* Decl. of Wendell Belew, ¶ 3. Plaintiff Ghafoor spoke over the telephone with al-Buthi approximately daily from February 19 through February 29, 2004 and approximately weekly thereafter. *See* Decl. of Asim Ghafoor, ¶ 3. Belew and Ghafoor were located in Washington D.C.; al-Buthi was located in Riyadh, Saudi Arabia. *See* Decl. of Wendell Belew, ¶ 3, Decl. of Asim Ghafoor, ¶ 3. The telephone number that Belew used was 202-255-3808; the telephone numbers that Ghafoor used were 202-390-5390, 202-497-2219 and 703-421-7303; the telephone numbers that al-Buthi used were 96655457679, 966506414004 and 966505457679. *See* Decl. of Wendell Belew, ¶ 3, Decl. of Asim Ghafoor, ¶ 3.

Al-Haramain and al-Buthi had been named among multiple defendants in *Burnett v. Al Baraka Investment and Development Corporation,* a lawsuit filed against Saudi Arabian entities and citizens on behalf of victims of the terrorist attacks of September 11, 2001. Al-Buthi was attempting to coordinate the defense of individuals named in the *Burnett* lawsuit and the payment of their legal fees. Al-Buthi contacted some of those individuals and urged them to obtain legal representation to prevent entry of default judgments against them. Ghafoor undertook to represent several of the individuals whom al-Buthi contacted. *See* Decl. of Asim Ghafoor, ¶ 4. Belew undertook to provide legal services in connection with the formation and operation of a lobbying organization for Islamic charities, the Friends of Charities Association (FOCA). *See* Decl. of Wendell Belew, ¶ 4.

Wholly independent of any classified written documentation, including the Sealed Document filed at the outset of this action, Belew and Ghafoor recall the substance of their telephone conversations with al-Buthi as follows:

- In the telephone conversations between Belew and al-Buthi, the parties discussed issues relating to the operation of FOCA, including the payment of FOCA's attorney fees to Belew and others. *See* Decl. of Wendell Belew, ¶ 5.

- In the telephone conversations between Ghafoor and al-Buthi, al-Buthi mentioned by name numerous defendants whom Ghafoor had undertaken to represent in the *Burnett* lawsuit filed on behalf of the September 11 victims. One of the names al-Buthi mentioned was Mohammad Jamal Khalifa, who was married to one of Osama bin-Laden's sisters. Two other names al-Buthi mentioned were Safar al-Hawali and Salman al-Auda, clerics whom Osama bin-Laden claimed had inspired him. *See* Decl. of Asim Ghafoor, ¶ 5.

- In the telephone conversations between Ghafoor and al-Buthi, the parties also discussed issues relating to payment of Ghafoor's legal fees as defense counsel in the *Burnett* lawsuit. *See id.*, ¶ 6.

F. Public evidence that defendants used classified documents in the 2004 investigation of Al-Haramain.

Public evidence demonstrates that defendants used classified documents in the 2004 investigation of Al-Haramain. In a letter to Al-Haramain's lawyer Lynne Bernabei dated April 23, 2004, OFAC Director Newcomb stated that OFAC was considering designating Al-Haramain as a Specially Designated Global Terrorist (SDGT) organization based on unclassified information "and on classified documents that are not authorized for public disclosure." *See* Decl. of Jon B. Eisenberg, exh. N at 70. In a follow-up letter to Bernabei dated July 23, 2004, Newcomb reiterated that OFAC was considering "classified information not being provided to you" in determining whether to designate Al-Haramain as an SDGT organization. *See id.*, exh. O at 72.

On September 9, 2004, OFAC declared Al-Haramain to be an SDGT organization. *See id.*, exh. P at 74. In a public declaration filed in the present litigation dated May 10, 2006, FBI Special Agent Frances R. Hourihan said the classified document that is the subject of this section 1806(f) motion "was related to the terrorist designation" of Al-Haramain. *See id.*, exh. Q at 77-78. In a letter to Al-Haramain's attorneys Lynne Bernabei and Thomas Nelson dated February 6, 2008, OFAC confirmed its "use of classified information" in the 2004 investigation. *See id.*, exh. R at 83, 85.

G. FBI Deputy Director Pistole's public admission that the FBI used surveillance in the 2004 investigation of Al-Haramain.

On October 22, 2007, in a speech at a conference of the American Bankers Association and American Bar Association on money laundering, the text of which appears on the FBI's official

Internet website, FBI Deputy Director Pistole stated that the FBI "used . . . surveillance" in connection with the 2004 investigation of Al-Haramain. *See id.*, exh. S at 92. In this speech, Pistole further stated that, although the FBI used surveillance in the investigation, "it was the financial evidence" provided by financial institutions "that provided justification for [Al-Haramain's] *initial* designation" on February 19, 2004. *See id.* (emphasis added).

Pistole's public admission that the FBI used surveillance in the Al-Haramain investigation contradicts defendants' prior assertion in their Brief for Appellants filed in the Ninth Circuit Court of Appeals in this litigation on June 6, 2007, that the government "could neither confirm nor deny whether plaintiffs had been surveilled under the TSP or any other intelligence-gathering program." *See id.*, exh. T at 98. With Pistole's speech and its posting on the FBI's website, the FBI has now publicly confirmed that plaintiffs were surveilled.

H. The inference that defendants used electronic surveillance of plaintiffs to declare links between Al-Haramain and Osama bin-Laden.

In a press release issued on September 9, 2004 – the day OFAC declared Al-Haramain to be an SDGT organization – the Treasury Department stated that the Al-Haramain investigation had shown "direct links between the U.S. branch [of Al-Haramain] and Usama bin Laden." *See id.*, exh. P at 74. This press release was the first instance of a public claim of purported links between Al-Haramain and Osama bin-Laden. The earlier press release of February 19, 2004, announcing the blocking of Al-Haramain's assets, did not mention Osama bin-Laden or al-Qaeda. *See id.*, exh. K at 54.

In a document filed in *United States v. Sedaghaty*, No. CR 05-60008-01 on August 21, 2007, the United States Attorney for the District of Oregon referred to the February 19, 2004 order blocking Al-Haramain's assets as a "preliminary designation" and referred to the September 9, 2004 order declaring Al-Haramain to be an SDGT as "a formal designation." *See* Decl. of Jon B. Eisenberg, exh. U at 102. Thus, in the government's own words, the assets-blocking order was "preliminary" (or, as Pistole put it in his speech, "initial") and the subsequent SDGT designation was "formal."

The timing of Belew's and Ghafoor's 2004 telephone conversations with al-Buthi, in which they discussed persons linked with Osama-bin Laden during the period between Al-Haramain's preliminary assets-blocking order and the formal SDGT designation, along with Pistole's admission

that the FBI surveilled Al-Haramain during this period, raise a compelling inference that defendants conducted electronic surveillance of those telephone conversations and then relied on that surveillance to declare links between Al-Haramain and Osama bin-Laden and issue the formal SDGT designation.

I. The public evidence that plaintiffs' surveillance was electronic.

FISA defines "electronic surveillance" in pertinent part as "the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States." 50 U.S.C. § 1801(f)(2). Defendant Alexander, CIA Director Michael Hayden, Director of National Intelligence Michael McConnell, and Assistant Attorney General Kenneth Wainstein have testified in various Senate and House committees that "[m]ost" telecommunications between the United States and abroad are transmitted by wire through routing stations located within the United States, from which the NSA intercepts such communications, so that their interception required a FISA warrant prior to the FISA Amendments Act of 2008, Pub. L. No. 110-261. *See* Decl. of Jon B. Eisenberg, exhs. V at 106, W at 111-114, X at 118, 120. This testimony demonstrates the probability that the 2004 telecommunications between al-Buthi and plaintiffs Belew and Ghafoor were wire communications intercepted within the United States, so that their interception was "electronic surveillance" within the meaning of FISA.

J. Other public evidence supporting the inference of electronic surveillance.

Other public evidence that supports the inference of plaintiffs' electronic surveillance includes the following:

- On June 12, 2006, during a district court hearing in *American Civil Liberties Union v. National Security Agency*, 493 F.3d 644 (6th Cir. 2007), Department of Justice Special Litigation Counsel Anthony Coppolino told the district judge that "attorneys who would represent terrorist clients . . . come closer to being in the ballpark with the terrorist surveillance program." *See* Decl. of Jon B. Eisenberg, exh. Y at 123-24. In defendants' Brief for Appellants filed in the Ninth Circuit Court, defendants described plaintiffs Al-Haramain, Belew and Ghafoor as "a terrorist organization, and two lawyers affiliated with Al-Haramain." *See id.*, exh. T at 97.

//

- Prior to 2004, defendants had conducted electronic surveillance of al-Buthi as revealed by a memorandum dated February 6, 2008, to defendant Szubin from Treasury Department Office of Intelligence and Analysis Deputy Assistant Secretary Howard Mendelsohn. The memorandum states that on February 1, 2003, the United States government conducted electronic surveillance of several telephone conversations between al-Buthi and Ali al-Timimi, and that these incidents of surveillance were publicly disclosed during al-Timimi's 2005 trial for allegedly soliciting persons to levy war against the United States. *See id.*, exh. Z at 130-131.

Given defendants' perception of Belew and Ghafoor as attorneys who "represent" and are "affiliated with" purported terrorists, along with defendants' admitted electronic surveillance of al-Buthi in the al-Timimi case, the electronic surveillance of Belew, Ghafoor and al-Buthi asserted in the present case should surprise nobody.

ARGUMENT

I. AS "AGGRIEVED PERSONS," PLAINTIFFS MAY OBTAIN ACCESS TO THE SEALED DOCUMENT UNDER APPROPRIATE SECURITY PROCEDURES AND PROTECTIVE ORDERS.

A. Whether plaintiffs may be given access to the sealed document turns on whether they can show they are "aggrieved" within the meaning of section 1806(f).

FISA section 1810 gives an "aggrieved person" a private right of action for electronic surveillance in violation of FISA. Plaintiffs' current challenge is to demonstrate their status as "aggrieved persons." As this Court has commented, "[s]ection 1810 is not user-friendly." Order in *Al-Haramain Islamic Foundation, Inc. v. Bush* (07-CV-109-VRW) (July 2, 2008) (Doc. 33), slip op. at 52 (hereinafter "Order of 7/2/08"). "The lack of precedents under section 1810 complicates the task of charting a path forward." *Id.*, slip op. at 56. This brief is intended to assist this Court in charting that path forward, specifically with regard to plaintiffs' use of section 1806(f) to gain access to the Sealed Document as part of their effort to establish standing.

We start with the basic proposition this Court has already enunciated – that "a litigant must first establish himself as an 'aggrieved person' before seeking to make a 'motion or request'" under section 1806(f) "'to discover or obtain applications or orders or other materials relating to electronic surveillance [etc.].'" Order of 7/2/08, slip op. at 48 (quoting 50 U.S.C. § 1806(f).) In the context of

the present case, that means "[p]laintiffs must first establish 'aggrieved person' status *without the use of the Sealed Document* and may then bring a 'motion or request' under § 1806(f) . . . ." *Id.*, slip op. at 49 (emphasis added). The issue here is whether the facts set forth in plaintiffs' amended complaint establish their "aggrieved person" status. If so, this motion lies for plaintiffs to obtain access to the Sealed Document. The threshold inquiry is what it means to be "aggrieved" under section 1806(f).

B. For plaintiffs to be "aggrieved" under section 1806(f), there must have been "surveillance" of plaintiffs and it must have been "electronic."

FISA itself answers the threshold question by defining "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*." 50 U.S.C. § 1801(k) (emphasis added). Under this statutory definition, there are only two requirements for a person to be aggrieved within the meaning of section 1806(f): There must have been *surveillance* of the person, and the surveillance must have been *electronic*.

Thus, section 1806(f)'s bar is low. By section 1801(k)'s definition, status as an "aggrieved person" to gain access to information under section 1806(f) is not the same as the broader requirement of *standing to sue* under FISA. Standing to sue requires *injury*. *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992). Electronic surveillance in and of itself is not injurious and thus is not actionable under section 1810. For there to be injury under section 1810, a third element must be present – the electronic surveillance must have been *warrantless* or have violated FISA in some other way.

The time has not yet come for this Court to determine whether plaintiffs' electronic surveillance was *warrantless*. For now, in order to adjudicate whether plaintiffs have made a sufficient showing under section 1806(f) to gain access to the Sealed Document, all this Court need decide is whether plaintiffs have made a sufficient showing that there was *surveillance* and that it was *electronic*.

When the time comes for this Court to adjudicate plaintiffs' standing and decide whether plaintiffs' electronic surveillance was warrantless, plaintiffs will argue two alternative points: First, the burden of proof must be shifted to *defendants* to show that the electronic surveillance was *not* warrantless – i.e., that it was authorized by a FISA warrant – because it is within defendants' exclusive

knowledge whether they had a FISA warrant. *See Campbell v. United States*, 365 U.S. 85, 96 (1961); *United States v. Denver & Rio Grande Railroad Company*, 191 U.S. 84, 92 (1903); *ITSI TV Productions, Inc. v. Agricultural Associations*, 3 F.3d 1289, 1292 (9th Cir. 1993). Second, and independent of this shifted burden of proof, the Sealed Document itself includes evidence that the electronic surveillance was warrantless.

But this Court's warrant determination will come later, when standing is adjudicated – which we anticipate will occur on a motion for summary adjudication of standing under Federal Rule of Civil Procedure 56(d). *See, e.g., Moreno v. Autozone, Inc.*, No. C05-04432 MJJ, 2007 WL 1063433, at *3 (N.D. Cal. Apr. 9, 2007) (holding summary adjudication is an appropriate procedure for determining standing). On the present motion, the only issue is whether there was electronic surveillance.

C. If plaintiffs show they are "aggrieved," this Court has discretion to give them access to the Sealed Document.

If this Court determines that plaintiffs have made a sufficient showing of electronic surveillance, the Court has *discretion* to give plaintiffs access to the Sealed Document. Section 1806(f) makes clear the discretionary nature of the Court's decision by stating that "the court *may* disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the . . . materials relating to the surveillance . . . ." 50 U.S.C. § 1806(f) (emphasis added).

Section 1806(f) authorizes discretionary disclosure "only where such disclosure is necessary to make an accurate determination of the legality of the surveillance." 50 U.S.C § 1806(f). Here, disclosure of the Sealed Document – under appropriate security procedures and protective orders – will assist this Court to make an accurate determination of the legality of plaintiffs' surveillance, for two reasons. First, the Sealed Document will help to nail down as indisputable, for purposes of showing standing, the prima facie case of electronic surveillance that plaintiffs have already presented. Second, the Sealed Document will help to supply the last link in the chain of evidence demonstrating plaintiffs' standing – the fact that plaintiffs' surveillance was warrantless – which will enable this Court to determine the legality of the surveillance.

//

//

II. PLAINTIFFS' BURDEN OF PROVING THEIR "AGGRIEVED PERSON" STATUS IS TO PRODUCE UNCLASSIFIED PRIMA FACIE EVIDENCE, DIRECT AND/OR CIRCUMSTANTIAL, SUFFICIENT TO RAISE A REASONABLE INFERENCE ON A PREPONDERANCE OF THE EVIDENCE THAT THEY WERE SUBJECTED TO ELECTRONIC SURVEILLANCE.

We next address the appropriate standard for determining whether a person is "aggrieved" for purposes of a motion to discover or obtain information under section 1806(f). This Court, in its order of July 2, 2008, said that "attempting a precise definition of such a standard is beyond the scope of this order." Order of 7/2/08, slip op. at 50. The time has now come to define that standard, on this motion under section 1806(f). We submit that plaintiffs' burden of proving their "aggrieved person" status is to produce unclassified prima facie evidence, direct and/or circumstantial, sufficient to raise a reasonable inference on a preponderance of the evidence that they were subjected to electronic surveillance.

A. The showing of "aggrieved" status need only be prima facie.

This court has noted two Ninth Circuit decisions – *United States v. See*, 505 F.2d 845 (9th Cir. 1974) and *United States v. Alter*, 482 F.2d 1016 (9th Cir. 1973) – arising under the Organized Crime Control Act, which establishes a procedure, prescribed in 18 U.S.C. section 3504(a)(1), by which "a party aggrieved" seeking to exclude illegally obtained evidence may obligate the government to affirm or deny the occurrence of the alleged unlawful act. We take these decisions as our starting point, in view of this Court's observation that they are "relevant," although not "directly transferable," to the determination of "aggrieved person" status under section 1806(f). Order of 7/2/08, slip op. at 50. The two decisions suggest a *prima facie* standard of proof.

On the one hand, according to *See*, a claim of electronic surveillance must be more than a "fishing expedition" in order to trigger section 3504(a)(1). 505 F.2d at 856. In the *See* prosecution, defendants moved for disclosure of purported electronic surveillance of defendant See's attorney two months previously. *Id.* at 849. The Ninth Circuit rejected defendants' "claim of unlawful surveillance *of them*" as being "vague to the point of being a fishing expedition," because defense counsel's supporting affidavit "did not allege that any electronic surveillance had been conducted in connection with the attorney's representation of *this defendant*." *Id.* at 856 (emphasis added). The *See* opinion indicates that, in civil FISA actions too, in order to establish "aggrieved person" status under section

1806(f), plaintiffs must produce evidence specifically connecting them with the alleged surveillance – i.e., showing that *they* were surveilled.

On the other hand, according to *Alter*, in order to trigger section 3504(a)(1), one "does not have to plead and prove his entire case." 482 F.2d at 1026. Rather, the appropriate standard of proof lies between the two extremes of an unsupported fishing expedition and indisputable proof: The plaintiff must "raise a prima facie issue of electronic surveillance." *Id.* In *Alter*, where a grand jury witness adjudged in civil contempt asserted the defense that his counsel had been subjected to unlawful surveillance, the court outlined the sort of evidence required to make the prima facie case: It includes "the specific facts which reasonably lead" to the belief there had been electronic surveillance, "the dates of such suspected surveillance," and "the identity of the person(s), by name or description, together with their respective telephone numbers . . . ." *Id. Alter* suggests that, in civil FISA actions too, in order to establish "aggrieved person" status under section 1806(f), plaintiffs need only produce prima facie evidence of electronic surveillance, including the sort of facts outlined in *Alter*.

A standard more demanding than prima facie proof would make nonsense of section 1806(f)'s provision for discovering or obtaining materials relating to electronic surveillance, by telling the plaintiffs: To get evidence that proves you were surveilled, you must first prove you were surveilled. Joseph Heller would be amused. But FISA is not a satirical novel. It is law, and it should mean something. As this Court put it, "the court must not interpret and apply FISA in a way that renders section 1810 superfluous." Order of 7/2/08, slip op. at 51-52. The provisions of section 1806(f) at issue here make sense only if interpreted as saying: To get access to materials that can help prove in a contested proceeding that you were surveilled, you must first make a prima facie case that you were surveilled.

Plaintiffs' showing of a prima facie case under section 1806(f) does *not* require this Court to determine any *contested facts* pertaining to the "surveillance" and "electronic" elements of "aggrieved person" status or the additional "warrantless" element of standing. A prima facie case is a one-sided affair – the *plaintiffs'* side. Thus, defendants cannot successfully oppose this section 1806(f) motion by presenting conflicting evidence with which they would hope to rebut the prima facie case. If defendants have any conflicting evidence to present, the time for that will come later, when this Court

adjudicates the broader issue of standing. At that time, if necessary, this Court can hold an evidentiary hearing to resolve any disputed factual issues. *See Bischoff v. Osceola County, Fla.*, 222 F.3d 874, 878-880 (11th Cir. 2000).

To make a prima facie case of electronic surveillance is certainly a daunting task, given the environment of secrecy in which electronic surveillance is normally conducted, but the task is not necessarily, as this Court has posited, "insurmountable." Order of 7/2/08, slip op. at 52. It can be accomplished under the extraordinary circumstances of the present case by applying traditional rules of civil proof to the unclassified evidence set forth in plaintiffs' amended complaint.

B. The showing may be made with circumstantial evidence.

Just last year, the D.C. Circuit decided *In re Sealed Case*, 494 F.3d 139 (D.C. Cir. 2007) – a *Bivens* action for electronic surveillance in violation of the Fourth Amendment – which helps to elucidate the appropriate standard of proof here. The issue in *In re Sealed Case* was whether the plaintiff was able to overcome the state secrets privilege by making a prima facie showing without using privileged information. In ruling for the plaintiff, the court enunciated two overarching principles (with which even a dissenting judge agreed, *id.* at 154) that should apply with equal force here.

First, the court said that a prima facie showing of electronic surveillance can be made with *circumstantial evidence*: "Although [the plaintiff's] case is premised on circumstantial evidence, '[a]s in any lawsuit, the plaintiff may prove his case by direct or circumstantial evidence.'" *Id.* at 147 (quoting *U.S. Postal Serv. Bd. of Governors v. Aikens*, 460 U.S. 711, 714 n.3 (1983)).

Defendants cannot quibble with this unremarkable proposition. Indeed, at a press conference on August 6, 2008, defendant FBI's Assistant Director Joseph Persechini stood at the side of U.S. Attorney for the District of Columbia Jeff Taylor as Taylor explained that circumstantial evidence against Dr. Bruce Ivins in the 2001 anthrax mailings would have proven his guilt beyond a reasonable doubt:

> [T]housands of prosecutors in thousands of courthouses prove cases beyond a reasonable doubt using circumstantial evidence. In fact, the standard jury instruction given by judges across the country is that a jury can consider circumstantial evidence and direct evidence, and they both can be given equal weight. . . . [I]t's compelling evidence and our view is we are confident it would have helped us prove this case against Dr. Ivins beyond a reasonable doubt.

See Decl. of Jon B. Eisenberg, exh. AA at 135. Based on that circumstantial evidence, an announcement on the FBI's official Internet website states: "Persichini was able to tell the American public that a chapter on one of the most heinous crimes committed against the citizens of the United States has been closed." *See id.*, exh. BB at 138.

If guilt beyond a reasonable doubt in a criminal prosecution can be proven with circumstantial evidence, then surely a prima facie showing of "aggrieved person" status for purposes of invoking section 1806(f) in a civil FISA action can be based on circumstantial evidence.

C. The showing is sufficient if it raises a reasonable inference of electronic surveillance.

The second overarching principle enunciated in *In re Sealed Case* is that a prima facie showing of electronic surveillance is sufficient if it raises a *reasonable inference* of electronic surveillance. The court explained that the plaintiff in that case was able to present unprivileged evidence "that creates an inference" of eavesdropping, evidence from which a jury could "reasonably infer that eavesdropping had occurred." 494 F.3d at 147.

Indeed, reasonable inference is embedded in the very notion of a prima facie case, which is commonly defined as "a party's production of enough evidence to allow the fact-trier to infer the fact at issue and rule in the party's favor." *Black's Law Dictionary* 1228 (8th ed. 2004).

D. The showing may be made on a preponderance of the evidence.

A third overarching principle – that the prima facie showing of electronic surveillance may be made on a *preponderance of the evidence* – appears in *American Civil Liberties Union v. National Security Agency*, 493 F.3d 644, where the plaintiffs asserted standing to sue under FISA on the ground their participation in international telecommunications for journalistic, legal and scholarly purposes made it likely they had been surveilled under the warrantless surveillance program. The court held that the plaintiffs had failed to demonstrate standing because "[t]he evidence establishes only a *possibility* – not a *probability* or certainty – that these communications might be intercepted." *Id.* at 674-75 (second emphasis added). "Probability" – the minimum showing the court required – means by a preponderance of the evidence.

//

In opposing a petition for a writ of certiorari in that case, the government stated that, to establish standing in a civil FISA action, "[p]roof by a preponderance of the evidence would suffice." *See* Decl. of Jon B. Eisenberg, exh. CC at 142. The government cannot now contend otherwise here.

We next show how plaintiffs' amended complaint meets their burden to present unclassified prima facie evidence, direct and/or circumstantial, sufficient to raise a reasonable inference on a preponderance of the evidence that they were subjected to electronic surveillance.

III. PLAINTIFFS HAVE MET THEIR BURDEN OF PROVING THEIR "AGGRIEVED PERSON" STATUS WITH THE UNCLASSIFIED INFORMATION SET FORTH IN THEIR AMENDED COMPLAINT.

A. The FBI has now publicly admitted that defendants used "surveillance" in the 2004 investigation of Al-Haramain.

Since the outset of this litigation in February of 2006, the public record has become replete with evidence of plaintiffs' surveillance in 2004. Much of this evidence is circumstantial, but not all of it: In October of 2007, the FBI publicly *admitted* – via Deputy Director Pistole's speech and its posting on the FBI's website – that defendants used surveillance in the 2004 investigation of Al-Haramain. *See supra* pp. 6-7.

So much for defendants' prior insistence in the Ninth Circuit that it is a state secret, vital to the Nation's security, "whether plaintiffs had been surveilled under the TSP or any other intelligence-gathering program." *See* Decl. of Jon B. Eisenberg, exh. T at 98, *supra* at 7. Despite telling the judiciary they cannot confirm or deny plaintiffs' surveillance without endangering national security, defendants subsequently touted that very surveillance to the public at large.

Now we know, via Pistole's admission, that defendants used surveillance in the 2004 investigation of Al-Haramain. But Pistole did not tell us *what* was surveilled. For that piece of the puzzle we must turn to other evidence.

B. Direct and circumstantial evidence raises a compelling inference that the 2004 surveillance of Al-Haramain included Belew's and Ghafoor's international telecommunications with al-Buthi.

Evidence made public since the inception of this litigation makes the case – not just prima facie, but compelling – that the surveillance Pistole admitted included Belew's and Ghafoor's 2004 telephone conversations with al-Buthi, where they discussed Ghafoor's representation of persons

linked with Osama bin-Laden and the payment of Belew's and Ghafoor's legal fees.

Here is what we know from public statements by defendants and other government officials, and from the declarations filed by Belew and Ghafoor in support of this motion, about the warrantless surveillance program and events during the 2004 investigation of Al-Haramain:

- Under the program, defendants surveilled international telecommunications of persons believed to be "linked" or "affiliated" with al-Qaeda. *See supra* p. 2.
- For several weeks starting on March 11, 2004, defendants conducted the program without DOJ certification and despite the Attorney General's advice that it was unlawful as then constituted. *See supra* p. 3.
- Upon the "preliminary designation" order blocking Al-Haramain's assets on February 19, 2004, defendants announced in a press release that they had begun investigating Al-Haramain, mentioning only possible crimes relating to currency and tax laws – with no mention of Osama bin-Laden or al-Qaeda. *See supra* p. 4.
- During this investigation, defendants used classified information produced by the intelligence community, and at that time the FBI was using information produced by the NSA under the warrantless surveillance program. *See supra* pp. 4, 6.
- In the midst of the investigation, in March and April of 2004, Belew and Ghafoor participated in international telecommunications where they discussed Ghafoor's representation of Al-Haramain and several persons linked with Osama bin-Laden. *See supra* pp. 5-6.
- Subsequently, on September 9, 2004, upon Al-Haramain's "formal designation" as an SDGT organization, defendants declared publicly that the investigation had shown "direct links" between Al-Haramain and Osama bin-Laden – the first instance of a claim of such links. *See supra* p. 6.

This unclassified evidence, which includes the "specific facts" required by *Alter*, 482 F.2d at 1026 (including the dates of the surveillance, the identities of the persons surveilled and their respective telephone numbers), raises the following inference: Defendants surveilled *Belew's and Ghafoor's international telecommunications with al-Buthi in March and April of 2004*, relying on that surveillance to issue the formal designation of Al-Haramain as an SDGT organization based on

purported "direct links" with Osama bin-Laden. A jury could reasonably infer from this evidence that the surveillance Pistole admitted included plaintiffs' international telecommunications. That inference is not just reasonable, it is compelling. It makes the prima case for the "surveillance" element of "aggrieved person" status under section 1806(f).

Other public evidence strengthens that inference even more. In the Ninth Circuit, defendants described Belew and Ghafoor as lawyers who are "affiliated with" a "terrorist organization." *See supra* p. 8. Mr. Coppolino has said that "attorneys who would represent terrorist clients . . . come closer to being in the ballpark with the terrorist surveillance program." *See supra* p. 8. Can it be any wonder that Belew's and Ghafoor's international telecommunications would be surveilled under a program that targeted persons the government perceived as "affiliated with" al-Qaeda and lawyers who represented so-called "terrorist clients"? Defendants have publicly admitted in the al-Timimi prosecution that they surveilled al-Buthi prior to 2004. *See supra* pp. 8-9. Can it be any wonder that they continued to surveil him in 2004?

C. Public statements by government officials demonstrate the probability that the 2004 surveillance was "electronic."

The prima facie case for the remaining element of "aggrieved person" status – the "electronic" nature of plaintiffs' surveillance – is made by the public statements of defendant Alexander, CIA Director Michael Hayden, Director of National Intelligence Michael McConnell, and Assistant Attorney General Kenneth Wainstein concerning how telecommunications between the United States and abroad are transmitted and intercepted: "Most" are transmitted by wire through routing stations located within the United States from which they are intercepted. *See supra* at 8. Their acquisition is thus "electronic" under FISA's definition of electronic surveillance as the acquisition of a "wire communication . . . if such acquisition occurs in the United States." 50 U.S.C. § 1801(f)(2).

These public statements do not indicate that *all* international telecommunications are transmitted by wire. But that is not necessary for plaintiffs to make their prima facie case. The case need only be made by a *preponderance of the evidence*, which means a *probability* – not a certainty – that plaintiffs' international telecommunications were transmitted by wire and were intercepted domestically. If that's how *most* international telecommunications are transmitted and intercepted,

then it is probable that's how *plaintiffs'* international telecommunications were transmitted and intercepted.

D. A "rich lode of disclosure" supports plaintiffs' prima facie case of electronic surveillance.

This Court has suggested that a "rich lode of disclosure" via unclassified evidence may be necessary to support plaintiffs' claim of electronic surveillance in order for them to gain access to the Sealed Document. Order of 7/2/08, slip op. at 51. We submit that plaintiffs have now met that standard, daunting though it is, through the confluence of government gaffes and public admissions as this litigation has unfolded. Upon the prima facie showing in plaintiffs' amended complaint, we request access to the Sealed Document, which FBI Special Agent Hourihan has said is "related to the terrorist designation" that arose from the electronic surveillance we have demonstrated. *See supra* p. 6.

The next step under section 1806(f) is for defendants to file an affidavit by the Attorney General asserting "that disclosure or an adversary hearing would harm the national security of the United States." 50 U.S.C. § 1806(f). If that happens, this Court must review the Sealed Document "in camera and ex parte . . . as may be necessary to determine whether [plaintiffs' surveillance] was lawfully authorized and conducted." *Id.* The Court may give plaintiffs access to portions of the Sealed Document "under appropriate security procedures and protective orders" as is "necessary to make an accurate determination of the legality of the surveillance." *Id.*

IV. PLAINTIFFS CAN SAFELY BE GIVEN ACCESS TO THE SEALED DOCUMENT USING SEVERAL POSSIBLE SECURITY MEASURES.

We propose several possible security measures by which plaintiffs can safely be given access to portions of the Sealed Document without endangering national security.

First, the Sealed Document can be *redacted* to prevent any public disclosure of sensitive information. Most of the document's contents are unnecessary to the showing of warrantless electronic surveillance. All we wish to use, for purposes of demonstrating standing, are portions of the document generally indicating or implying that defendants intercepted plaintiffs' international telecommunications in March and April of 2004 and lacked a warrant to do so. Any and all information in the document concerning the operational details of the interception is unnecessary to

show plaintiffs' standing and can be redacted in the interests of national security.

Second, as prescribed by section 1806(f), this Court can issue a *protective order* – the violation of which can be made punishable by contempt proceedings – prohibiting plaintiffs and their counsel from publicly disclosing any of the Sealed Document's contents. Such an order has never been necessary here – throughout the two and a half years of this litigation, and going back to the Sealed Document's accidental disclosure in 2004, plaintiffs and their counsel have been scrupulously careful never to breathe a public word about the document's contents. We take seriously our obligations to protect the Sealed Document from unauthorized disclosure – not to mention that such disclosure would be a crime. *See* 18 U.S.C. § 793. Nevertheless, a protective order by this Court will add another layer of safety – on top of our own respect for national security and the law against unauthorized disclosure – and we will comply with it.

Third, defendants can give one or more of plaintiffs' counsel access to the Sealed Document under a strict security clearance with conditions of defendants' choosing which will further ensure against unauthorized public disclosure of the document's contents. This will add yet another layer of protection, given the consequences counsel would suffer for violating the security clearance. Three attorneys and a paralegal at the Center for Constitutional Rights, the plaintiff in another pending MDL case challenging the warrantless surveillance program (*Center for Constitutional Rights v. Bush, et al.*), have been given Top Secret/Sensitive Compartmented Information (TS/SCI) clearances, which evidently took only six weeks to process and complete, in connection with their litigation of cases against the U.S. Government on behalf of individuals detained at Guantanamo Bay, Cuba. *See* Decl. of Shayana Kadidal. There is no reason why the same cannot be done here.

Finally, we note that the "access" we seek is not a first-time "disclosure" of the Sealed Document in the broad sense of us never having seen it previously, for we have already seen it. Rather, we seek disclosure in the much narrower sense of this Court simply acknowledging the Sealed Document's existence and permitting us to access portions of it and then reference it – e.g., in a sealed memorandum of points and authorities – in our arguments on subsequent proceedings to determine plaintiffs' standing. National security cannot possibly be threatened by allowing us to see and tell this Court, in confidence, what we already have seen and know.

CONCLUSION

For the foregoing reasons, we respectfully request this Court to grant this motion under section 1806(f) and give us access to the Sealed Document under such security conditions and protective orders as the Court deems appropriate.

DATED this 30th day of September, 2008.

/s/ Jon B. Eisenberg

Jon B. Eisenberg, Calif. Bar No. 88278
William N. Hancock, Calif. Bar No. 104501
Steven Goldberg, Ore. Bar No. 75134
Thomas H. Nelson, Oregon Bar No. 78315
Zaha S. Hassan, Calif. Bar No. 184696
J. Ashlee Albies, Ore. Bar No. 05184
Lisa Jaskol, Calif. Bar No. 138769

Attorneys for Plaintiffs Al-Haramain Islamic Foundation, Inc., Wendell Belew, and Asim Ghafoor