	12235e1\8:067-cv-00071999-VIRW Documment 5377 Hited0011055220099 Heage 11061225
1	
2	
2	
4	
5	IN THE UNITED STATES DISTRICT COURT
6	FOR THE NORTHERN DISTRICT OF CALIFORNIA
7	
, 8	
9	IN RE: MDL Docket No 06-1791 VRW
10	NATIONAL SECURITY AGENCY ORDER TELECOMMUNICATIONS RECORDS
11	LITIGATION
12	This order pertains to:
13	Al-Haramain Islamic Foundation et al v Bush et al (C 07-0109 VRW),
14	
15	
16	On November 16, 2007, the court of appeals remanded this
17	case for this court to consider whether the Foreign Intelligence
18	Surveillance Act, 50 USC §§ 1801-71, ("FISA") "preempts the state
19	secrets privilege and for any proceedings collateral to that
20	determination." Al-Haramain Islamic Foundation, Inc v Bush, 507
21	F3d 1190, 1206 (9th Cir 2007). This court entertained briefing and
22	held a hearing on that issue and, on July 2, 2008, issued a ruling
23	that: (1) FISA preempts the state secrets privilege in connection
24	with electronic surveillance for intelligence purposes and would
25	appear to displace the state secrets privilege for purposes of
26	plaintiffs' claims; and (2) FISA did not appear to provide
27	plaintiffs with a viable remedy unless they could show that they
28	were "aggrieved persons" within the meaning of FISA. In re

.

1 National Security Agency Telecommunications Records Litigation, 564 2 F Supp 2d 1109, 1111 (N D Cal 2008). The court dismissed the 3 complaint with leave to amend. Plaintiffs timely filed an amended pleading (Doc #458/35<sup>1</sup>) and defendants, for the third time, moved 4 5 to dismiss (Doc #475/49). Plaintiffs simultaneously filed a motion 6 to "discover or obtain material relating to electronic 7 surveillance" under 50 USC § 1806(f) (Doc #472/46), which 8 defendants oppose (Doc #496/50).

9 This pair of cross-motions picks up, at least in theory, 10 where the court's July 2, 2008 order left off. At issue on these 11 cross-motions is the adequacy of the first amended complaint (Doc 12 #35/458)("FAC") to enable plaintiffs to proceed with their suit. 13 Accordingly, the court's discussion will address the motions 14 together.<sup>2</sup>

16

15

24

Ι

As with the original complaint, plaintiffs are the Al-Haramain Islamic Foundation, Inc, an Oregon non-profit corporation ("Al-Haramain Oregon"), and two of its individual attorneys, Wendell Belew and Asim Ghafoor, both United States citizens ("plaintiffs"). Plaintiffs sue generally the same defendants but replace one office-holder with his replacement, make minor punctuation and wording changes and specify that they are suing one

<sup>&</sup>lt;sup>25</sup> <sup>1</sup> Documents will cited both to the MDL docket number (No M 06-1791) and to the individual docket number (No C 07-0109) in the <sup>26</sup> following format: Doc #xxx/yy.

<sup>27 &</sup>lt;sup>2</sup> These motions do not implicate the recent amendments to FISA enacted after the July 2 order (FISA Amendments Act of 2008, Pub L No 110-261, 122 Stat 2436 (FISAAA), enacted July 10, 2008).

defendant in both his official and personal capacities: "George W Bush, President of the United States, National Security Agency and Keith B Alexander, its Director; Office of Foreign Assets Control, an office of the United States Treasury, and Adam J Szubin, its Director; Federal Bureau of Investigation and Robert S Mueller, III, its Director, in his official and personal capacities" ("defendants").

8 The FAC retains the same six causes of action as the 9 original complaint. First, plaintiffs allege a cause of action 10 under FISA that encompasses both a request, under 50 USC § 1806(g), for suppression of evidence obtained through warrantless electronic 11 12 surveillance and a claim for damages under § 1810. Doc #458/35 at 13 Then, plaintiffs allege violations of the following 14. 14 Constitutional provisions: the "separation of powers" principle 15 (i e, that the executive branch has exceeded its authority under Article II); the Fourth Amendment through warrantless surveillance 16 17 of plaintiffs' electronic communications; the First Amendment through warrantless surveillance, impairing plaintiffs' "ability to 18 19 obtain legal advice, to freely form attorney-client relationships, 20 and to petition the government \* \* \* for redress of grievances 21 \* \* \*"; and the Sixth Amendment through surveillance of plaintiffs' 22 electronic communications without probable cause or warrants. Id 23 at 14-15. And finally, plaintiffs allege violations of the 24 International Covenant on Civil and Political Rights. Id at 15-16.

In drafting the FAC, plaintiffs have greatly expanded their factual recitation, which now runs to ten pages (id at 3-12), up from a little over one page. The FAC recites in considerable detail a number of public pronouncements of government officials 1 about the Terrorist Surveillance Project ("TSP") and its 2 surveillance activities as well as events publicly known about the 3 TSP including a much-publicized hospital room confrontation between 4 former Attorney General John Ashcroft and then-White House counsel 5 (later Attorney General) Alberto Gonzales (id at 5).

Of more specific relevance to plaintiffs' effort to
allege sufficient facts to establish their "aggrieved person"
status, the FAC also recites a sequence of events pertaining
directly to the government's investigations of Al-Haramain Oregon.
A slightly abbreviated version of these allegations follows:

11 On August 1, 2002, Treasury Department Deputy Secretary 12 Kenneth W Dam testified in Congress that, in October of 2001, the 13 Treasury Department created "Operation Green Quest" to track 14 financing of terrorist activities, one of the targets of which were 15 foreign branches of the Saudi Arabia-based Al-Haramain Islamic 16 Foundation. ¶ 24.

On March 4, 2004, FBI Counterterrorism Division Acting 17 18 Assistant Director Gary M Bald testified in Congress that: in April 19 of 2002, the FBI created its Terrorist Financing Operations Section 20 (TFOS); on May 13, 2003, through a Memorandum of Understanding 21 between the Department of Justice and the Department of Homeland 22 Security, the FBI was designated as the lead Department to 23 investigate potential terrorist-related financial transactions; the 24 TFOS acquired, analyzed and disseminated classified electronic 25 intelligence data, including telecommunications data from sources 26 in government and private industry; TFOS took over the 27 investigation of Al-Haramain Islamic Foundation "pertaining to 28 terrorist financing"; on February 18, 2004, the FBI executed a

search warrant on plaintiff Al-Haramain Oregon's office in Ashland, Oregon; and TFOS provided operational support, including document and data analysis, in the investigation of plaintiff Al-Haramain Oregon. ¶ 25. Bald's March 4, 2004 testimony included no mention of purported links between plaintiff Al-Haramain Oregon and Osama bin-Laden. ¶ 26.

7 On September 25, 2003, FBI Deputy Director John S Pistole 8 testified in Congress that the TFOS "has access to data and 9 information" from "the Intelligence Community" and has "[t]he 10 ability to access and obtain this type of information in a time 11 sensitive and urgent manner." ¶ 27.

12 On June 16, 2004, OFAC Director R Richard Newcomb 13 testified in Congress that in conducting investigations of 14 terrorist financing, OFAC officers use "classified \* \* \* 15 information sources." ¶ 28.

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.

On February 19, 2004, the Treasury Department issued a press release announcing that OFAC had blocked Al-Haramain Oregon's assets pending an investigation of possible crimes relating to currency reporting and tax laws; the document contained no mention of purported links between plaintiff Al-Haramain Oregon and Osama bin-Laden. ¶¶ 30-31.

26 Soon after the blocking of plaintiff Al-Haramain Oregon's 27 assets on February 19, 2004, plaintiff Belew spoke by telephone 28 with Soliman al-Buthi (alleged to be one of Al-Haramain Oregon's

1 directors) on the following dates: March 10, 11 and 25, April 16, 2 May 13, 22 and 26, and June 1, 2 and 10, 2004. Belew was located 3 in Washington DC; al-Buthi was located in Riyadh, Saudi Arabia. During the same period, plaintiff Ghafoor spoke by telephone with 4 5 al-Buthi approximately daily from February 19 through February 29, 6 2004 and approximately weekly thereafter. Ghafoor was located in 7 Washington DC; al-Buthi was located in Riyadh, Saudi Arabia. (The 8 FAC includes the telephone numbers used in the telephone calls 9 referred to in this paragraph.) ¶¶ 34-35.

10 In the telephone conversations between Belew and al-11 Buthi, the parties discussed issues relating to the legal 12 representation of defendants, including Al-Haramain Oregon, named in a lawsuit brought by victims of the September 11, 2001 attacks. 13 Names al-Buthi mentioned in the telephone conversations with 14 15 Ghafoor included Mohammad Jamal Khalifa, who was married to one of Osama bin-Laden's sisters, and Safar al-Hawali and Salman al-Auda, 16 17 clerics whom Osama bin-Laden claimed had inspired him. In the 18 telephone conversations between Ghafoor and al-Buthi, the parties 19 also discussed logistical issues relating to payment of Ghafoor's 20 legal fees as defense counsel in the lawsuit. Id.

21 In a letter to Al-Haramain Oregon's lawyer Lynne Bernabei 22 dated April 23, 2004, OFAC Director Newcomb stated that OFAC was 23 considering designating Al-Haramain Oregon as a Specially 24 Designated Global Terrorist (SDGT) organization based on 25 unclassified information "and on classified documents that are not 26 authorized for public disclosure." ¶ 36. In a follow-up letter to 27 Bernabei dated July 23, 2004, Newcomb reiterated that OFAC was 28 considering "classified information not being provided to you" in

determining whether to designate Al-Haramain Oregon as an SDGT
 organization. ¶ 37. On September 9, 2004, OFAC declared plaintiff
 Al-Haramain Oregon to be an SDGT organization. ¶ 38.

In a press release issued on September 9, 2004, the Treasury Department stated that the investigation of Al-Haramain Oregon showed "direct links between the US branch [of Al-Haramain] and Usama bin Laden"; this was the first public claim of purported links between Al-Haramain Oregon and Osama bin-Laden. ¶¶ 39-40.

9 In a public declaration filed in this litigation dated 10 May 10, 2006, FBI Special Agent Frances R Hourihan stated that a 11 classified document "was related to the terrorist designation" of 12 Al-Haramain Oregon.

13 On October 22, 2007, in a speech at a conference of the American Bankers Association and American Bar Association on money 14 15 laundering, the text of which appears on the FBI's official Internet website, FBI Deputy Director Pistole stated that the FBI 16 "used \* \* \* surveillance" in connection with defendant OFAC's 2004 17 18 investigation of Al-Haramain Oregon but that "it was the financial 19 evidence" provided by financial institutions "that provided 20 justification for the initial designation" of Al-Haramain Oregon. 21  $\P\P$  42-43. A court document filed by the United States Attorney for 22 the District of Oregon on August 21, 2007 referred to the February 23 19, 2004 asset-blocking order as a "preliminary designation" and 24 the September 9, 2004 order as "a formal designation." **44**.

To allege that the above-referenced telecommunications
between al-Buthi and plaintiffs Belew and Ghafoor were wire
communications and were intercepted by defendants within the United
States, plaintiffs cite in their FAC several public statements by

1 government officials, including: July 26, 2006 testimony by 2 defendant Alexander and CIA Director Michael Hayden that 3 telecommunications between the United States and abroad pass through routing stations located within the United States from 4 5 which the NSA intercepts such telecommunications; May 1, 2007 testimony by Director of National Intelligence Mike McConnell that 6 7 interception of surveilled electronic communications between the 8 United States and abroad occurs within the United States and thus 9 requires a warrant under FISA; September 20, 2007 testimony by McConnell testified before the House Select Intelligence Committee 10 11 that "[t]oday \* \* \* [m]ost international communications are on a 12 wire, fiber optical cable," and "on a wire, in the United States, 13 equals a warrant requirement [under FISA] even if it was against a foreign person located overseas." ¶ 48a-c. 14

A memorandum dated February 6, 2008, to defendant Szubin from Treasury Department Office of Intelligence and Analysis Deputy Assistant Secretary Howard Mendelsohn, which was publicly disclosed during a 2005 trial, acknowledged electronic surveillance of four of Al-Buthi's telephone calls with an individual unrelated to this case on February 1, 2003. ¶ 51.

21 In support of their motion under § 1806(f), plaintiffs 22 submit evidence substantiating the allegations of their FAC. In 23 addition to numerous documents drawn from United States government 24 websites and the websites of news organizations (Exhibits to Doc 25 #472-1/46-1, passim), plaintiffs submit the sworn declarations of 26 plaintiffs Wendell Belew and Asim Ghafoor attesting to the 27 specifics and contents of the telephone conversations described in 28 paragraphs 32 and 33 of the FAC. Doc ##472-6/46-6, 472-7/46-7.

II

2 Defendants' papers attack the sufficiency of plaintiffs' 3 allegations in their FAC and the evidence presented in their motion under § 1806(f) to establish that they are "aggrieved persons" 4 5 under FISA and thereby have standing to utilize the special procedures set forth in § 1806(f) of FISA to investigate the 6 7 alleged warrantless surveillance and to seek civil remedies under 8 § 1810. An "aggrieved person" under FISA is defined in 50 USC 9 §1801(k) as the "target of an electronic surveillance" or a person "whose communications or activities were subject to electronic 10 11 surveillance." Defendants contend that "nothing in the [FAC] comes 12 close to establishing that plaintiffs are 'aggrieved persons' under 13 FISA and thus have standing to proceed under Section 1806(f) to litigate any claim." Doc #475/49 at 6. 14

15 Plaintiffs' motion, by contrast, asserts that the FAC presents "abundant unclassified information demonstrating 16 17 plaintiffs' electronic surveillance in March and April of 2004" 18 and, on that basis, seeks a determination of "aggrieved person" 19 status under FISA. Plaintiffs also "propose several possible 20 security measures by which plaintiffs can safely be given access to 21 portions of" the classified document that was accidentally revealed 22 to plaintiffs during discovery and returned under orders of the 23 Oregon District Court (the "Sealed Document") and which has been 24 the subject of considerable attention in this litigation. Doc 25 #472/46 at 5-6.

- 26 \\
- 27 \\
- 28 \\

Α

1 2 Both FISA sections under which plaintiffs seek to 3 proceed, §§ 1810 and 1806(f), are available only to "aggrieved persons" as defined in 50 USC § 1801(k). The court's July 2 order 4 5 discussed the lack of precedents under FISA and devoted 6 considerable space to opinions applying 18 USC § 3504(a)(1), 7 governing litigation concerning sources of evidence. 564 F Supp 2d 8 at 1133-35. The Ninth Circuit's standards under § 3504(a)(1), 9 while not directly transferrable to FISA, appear to afford a source 10 of relevant analysis to use by analogy in interpreting FISA, 11 subject to that statute's national-security-oriented context: 12 The flexible or case-specific standards articulated by the Ninth Circuit for establishing aggrieved status under 13 section 3504(a)(1), while certainly relevant, do not appear directly transferrable to the standing inquiry for 14 an "aggrieved person" under FISA. While attempting a precise definition of such a standard is beyond the scope 15 of this order, it is certain that plaintiffs' showing thus far with the Sealed Document excluded falls short of 16 the mark. 17 Plaintiff amici hint at the proper showing when they refer to "independent evidence disclosing that plaintiffs 18 have been surveilled" and a "rich lode of disclosure to support their claims" in various of the MDL cases. \* \* \* 19 To proceed with their FISA claim, plaintiffs must present 20 to the court enough specifics based on non-classified evidence to establish their "aggrieved person" status 21 under FISA. Id at 1135. 22 23 Defendants' opening brief (Doc #475/49) largely fails to 24 engage with the question posed by the court, instead reiterating 25 standing arguments made previously (at 16-17) and asserting that 26 "the law does not support an attempt to adjudicate whether the 27 plaintiffs are 'aggrieved persons' in the face of the Government's 28 successful state secrets privilege assertion" (at 27-30).

1 Defendants advance one apparently new argument in this regard: that the adjudication of "aggrieved person" status for any or all 2 3 plaintiffs cannot be accomplished without revealing information protected by the state secrets privilege ("SSP"). 4 This argument 5 rests on the unsupported assertion that "[t]he Court cannot 6 exercise jurisdiction based on anything less than the actual facts" 7 (id at 28), presumably in contrast to inferences from other facts 8 (on which defendants contend the FAC exclusively relies). 9 Defendants' position boils down to this: only affirmative 10 confirmation by the government or equally probative evidence will meet the "aggrieved person" test; the government is not required to 11 12 confirm surveillance and the information is not otherwise available without invading the SSP. In defendants' view, therefore, 13 plaintiffs simply cannot proceed on their claim without the 14 15 government's active cooperation — and the government has evinced no intention of cooperating here. 16

17 Defendants' stance does not acknowledge the court's 18 ruling in the July 2, 2008 order that FISA "preempts" or displaces 19 the SSP for matters within its purview and that, while obstacles 20 abound, canons of construction require that the court avoid 21 interpreting and applying FISA in a way that renders FISA's § 1810 22 superfluous. Accordingly, the court ruled, there must be some 23 legally sufficient way to allege that one is an "aggrieved person" 24 under § 1801(k) so as to survive a motion to dismiss. Of note, 25 defendants also continue to maintain, notwithstanding the July 2 26 rulings, that the SSP requires dismissal and that FISA does not 27 preempt the SSP. They also suggest that appellate review of the 28 preemption ruling and several of the issues implicated in the

1 instant motions might be "appropriate" if the court decides to 2 proceed under § 1806(f). Doc #475/49 at 31. (Plaintiffs counter 3 that an interlocutory appeal of the preemption question would not 4 be timely. Doc #496/50 at 28).

5 Plaintiffs urge the court to adopt the Ninth Circuit's prima facie approach under 18 USC § 3504(a)(1) set forth in United 6 7 States v Alter, 482 F2d 1016 (9th Cir 1973), that is, that a prima 8 facie case of electronic surveillance requires "evidence 9 specifically connecting them with the surveillance --- i e showing that they were surveilled" without requiring that they "plead and 10 prove [their] entire case." Plaintiffs further suggest that the 11 12 prima facie case does not require the determination of any 13 contested facts but rather is "a one-sided affair - the 14 plaintiff's side." Doc #472/46 at 20.

15 Plaintiffs also point to the DC Circuit's recent decision in In Re Sealed Case, 494 F 3d 139 (DC Cir 2007), which reversed 16 17 the district court's dismissal of a Bivens action by a Drug Enforcement Agency employee based on the government's assertion of 18 19 the SSP. The district court had concluded that the plaintiff's 20 unclassified allegations of electronic eavesdropping in violation 21 of the Fourth Amendment were insufficient to establish a prima 22 facie case. Id at 147. The DC Circuit upheld the dismissal as to 23 a defendant called "Defendant II" of whom the court wrote "nothing 24 about this person would be admissible in evidence at trial," but 25 reversed the dismissal as to defendant Huddle, noting that although 26 plaintiff's case "is premised on circumstantial evidence 'as in any 27 lawsuit, the plaintiff may prove his case by direct or 28 circumstantial evidence.'" Id. Plaintiffs accordingly argue that

circumstantial evidence of electronic surveillance should be sufficient to establish a prima facie case. The court agrees with plaintiffs that this approach comports with the intent of Congress in enacting FISA as well as concepts of due process which are especially challenging — but nonetheless especially important to uphold in cases with national security implications and classified evidence.

8 Plaintiffs articulate their proposed standard, in 9 summary, as follows: "plaintiffs' burden of proving their 10 'aggrieved person' status is to produce unclassified prima facie 11 evidence, direct and/or circumstantial, sufficient to raise a 12 reasonable inference on a preponderance of the evidence that they 13 were subjected to electronic surveillance." Doc #472/46 at 19.

14 Defendants attack plaintiffs' proposed prima facie case approach by suggesting, as to plaintiffs' motion, that "no court 15 has ever used Section 1806(f) in this manner" and that it would 16 17 "open a floodgate of litigation whereby anyone who believes he can 18 'infer' from 'circumstantial evidence' that he was subject to 19 electronic surveillance could compel a response by the Attorney 20 General under Section 1806(f) and seek discovery of the matter 21 through ex parte, in camera proceedings." Doc # 499/51 at 12-13. 22 These points are without merit.

The lack of precedents for plaintiffs' proposed approach is not meaningful given the low volume of FISA litigation in the thirty years since FISA was first enacted. It is, moreover, unlikely that this court's order allowing plaintiffs to proceed will prompt a "flood" of litigants to initiate FISA litigation as a means of learning about suspected unlawful surveillance of them by

1 the government. And finally, the court has ruled that allegations 2 sufficient to allege electronic surveillance under FISA must be, to 3 some degree, particularized and specific, a ruling that discourages 4 weakly-supported claims of electronic surveillance. <u>In re National</u> 5 Security Agency, 564 F Supp 2d at 1135.

In <u>Alter</u>, the Ninth Circuit specifically noted the
competing considerations and special challenges for courts in cases
of alleged electronic surveillance:

We \* \* \* seek to create a sound balance among the competing demands of constitutional safeguards protecting the witness and the need for orderly grand jury processing. We do not overlook the intrinsic difficulty in identifying the owner of an invisible ear; nor do we discount the need to protect the Government from unwarranted burdens in responding to ill-founded suspicions of electronic surveillance.

14 482 F2d at 1026. The prima facie approach employed by the Ninth 15 Circuit fairly balances the important competing considerations at work in electronic surveillance cases. Its stringency makes it 16 17 appropriate in cases arising in the somewhat more restrictive 18 litigation environment where national security dimensions are 19 The DC Circuit's recent use of a prima facie approach in present. 20 such a case underscores that this is a proper manner in which to 21 In re Sealed Case, 494 F 3d 139. It appears consistent, proceed. 22 moreover, with the intent of Congress in enacting FISA's sections 23 1810 and 1806(f).

в

Defendants devote considerable space to their argument that plaintiffs have not established "Article III standing." E g, Doc #475/49 at 17. In support of this contention, they largely re-

9

10

11

12

13

24

25

1 hash and re-purpose the standing arguments made in support of their 2 previous two motions to dismiss.

3 The court will limit its discussion of this issue to defendants' reliance on Alderman v United States, 394 US 165 4 5 (1969), which they cite in all of their briefs on these motions in 6 support of their contention that plaintiffs lack standing. Doc 7 #475/49 at 17; Doc # 499/51 at 9, 10, 26 and 27; Doc #516/54 at 9. 8 In Alderman, the Supreme Court considered, in connection with legal 9 challenges brought under the Fourth Amendment, "the question of standing to object to the Government's use of the fruits of illegal 10 surveillance" in criminal prosecutions. Id at 169. 11 Explaining 12 that "[w]e adhere to \* \* \* the general rule that Fourth Amendment 13 rights are personal rights which, like some other constitutional rights, may not be vicariously asserted," the Court held that the 14 15 Fourth Amendment protects not only the private conversations of individuals subjected to illegal electronic surveillance, but also 16 17 the owner of the premises upon which the surveillance occurs. 18 While the Court made mention of the then-recently-enacted Omnibus 19 Crime Control and Safe Streets Act of 1968 codified at chapter 119 20 of Title 18 of the United States Code, 18 USC §§ 2510-22 ("Title 21 III"), Alderman did not arise under Title III.

The footnote about standing that defendants repeatedly cite on the instant motions merely amplified the statement in the text of <u>Alderman</u> that "Congress or state legislatures may extend the exclusionary rule and provide that illegally seized evidence is inadmissible against anyone for any purpose," with the observation that Congress had <u>not</u> provided for such an expansion of standing to suppress illegally intercepted communications in Title III. Id at

1 175 & n9. Defendants' reliance on Alderman is somewhat baffling 2 because here, the individuals who were allegedly subjected to the 3 warrantless electronic surveillance are parties to the lawsuit and are specifically seeking relief under provisions of FISA intended 4 5 to provide remedies to individuals subjected to warrantless 6 electronic surveillance. The disposition in Alderman further 7 undermines defendants' broader contention that only acknowledged 8 warrantless surveillance confers standing: the Court remanded the 9 cases to the district court for "a hearing, findings, and 10 conclusions" whether there was electronic surveillance that violated the Fourth Amendment rights of any of the petitioners and, 11 12 if so, as to the relevance of the surveillance evidence to the 13 criminal conviction at issue. Id at 186.

14 The court declines to entertain further challenges to plaintiffs' standing; the July 2 order (at 1137) gave plaintiffs 15 the opportunity to "amend their claim to establish that they are 16 17 'aggrieved persons' within the meaning of 50 USC § 1801(k)." 18 Plaintiffs have alleged sufficient facts to withstand the 19 government's motion to dismiss. To quote the Ninth Circuit in 20 Alter, "[t]he [plaintiff] does not have to plead and prove his 21 entire case to establish standing and to trigger the government's 22 responsibility to affirm or deny." 482 F2d at 1026. Contrary to 23 defendants' assertions, proof of plaintiffs' claims is not 24 necessary at this stage. The court has determined that the 25 allegations "are sufficiently definite, specific, detailed, and 26 nonconjectural, to enable the court to conclude that a substantial 27 claim is presented." Id at 1025.

28

 $\boldsymbol{1}$ 

Document 537 235618:06-cv-00799-VRW Hiledol 1055220099 Hage 17706 1225 C 1 2 Defendants summarize plaintiffs' allegations thusly, 3 asserting that they are "obviously" insufficient "under any standard": 4 5 the sum and substance of plaintiffs' factual allegations are that: (i) the [TSP] targeted 6 communications with individuals reasonably believed to be associated with al Qaeda; (ii) in February 2004, the 7 Government blocked the assets of AHIF-Oregon based on its association with terrorist organizations; (iii) in 8 March and April of 2004, plaintiffs Belew and Ghafoor talked on the phone with an officer of AHIF-Oregon in 9 Saudi Arabia (Mr al-Buthe [sic]) about, inter alia, persons linked to bin-Laden; (iv) in the September 2004 10 designation of AHIF-Oregon, [OFAC] cited the organization's direct links to bin-Laden as a basis for 11 the designation; (v) the OFAC designation was based in part on classified evidence; and (vi) the FBI stated it 12 had used surveillance in an investigation of the Al-Haramain Islamic Foundation. Plaintiffs specifically 13 allege that interception of their conversations in March and April 2004 formed the basis of the September 2004 designation, and that any such interception was 14 electronic surveillance as defined by the FISA 15 conducted without a warrant under the TSP. Doc #516/54 at 12 (citations to briefs omitted). 16 17 The court does not find fault with defendants' summary 18 but disagrees with defendants' sense of the applicable legal 19 standard. Defendants seem to agree that legislative history and 20 precedents defining "aggrieved person" from the Title III context 21 may be relevant to the FISA context (Doc #475/49 at 17 n 3), but 22 argue that "Congress incorporated Article III standing requirements 23 in any determination as to whether a party is an 'aggrieved person' 24 under the FISA" (Doc #516/54 at 7) and assert that "the relevant 25 case law makes clear that Congress intended that `aggrieved 26 persons' would be solely those litigants that meet Article III 27 standing requirements to pursue Fourth Amendment claims." Id at 5. 28 Tellingly, defendants in their reply brief consistently refer to

United States District Court For the Northern District of California 1 their motion as a "summary judgment motion" and argue that 2 plaintiffs cannot sustain their burden on "summary judgment" based 3 on the allegations of the FAC. Defendants are getting ahead of 4 themselves.

5 Defendants attack plaintiffs' FAC by asserting that plaintiffs seek to proceed with the lawsuit based on "reasonable 6 7 inferences" and "logical probabilities" but that they cannot avoid 8 summary judgment because "their evidence does not actually 9 establish that they were subject to the alleged warrantless 10 surveillance that they challenge in this case." Id at 11. At oral argument, moreover, counsel for defendants contended that the only 11 12 way a litigant can sufficiently establish aggrieved person status 13 at the pleading stage is for the government to have admitted the 14 unlawful surveillance. Transcript of hearing held December 2, 15 2008, Doc #532 at 5-17.

16 Without a doubt, plaintiffs have alleged enough to plead 17 "aggrieved person" status so as to proceed to the next step in 18 proceedings under FISA's sections 1806(f) and 1810. While the 19 court is presented with a legal problem almost totally without 20 directly relevant precedents, to find plaintiffs' showing 21 inadequate would effectively render those provisions of FISA 22 without effect, an outcome the court is required to attempt to 23 avoid. See In re National Security Agency, 564 F Supp 2d at 1135 24 ("While the court must not interpret and apply FISA in way that 25 renders section 1810 superfluous, Dole Food Co v Patrickson, 538 US 26 468, 476-77, 123 S Ct 1655 (2003), the court must be wary of 27 unwarranted interpretations of FISA that would make section 1810 a 28 more robust remedy than Congress intended it to be.") More

(	CasselV3::067-cv-0107199-VIRW Documment 537 Filided0011055220099 Fizage 199061225
1	importantly, moreover, plaintiffs' showing is legally sufficient
2	under the analogous principles set forth in <u>Alter</u> and <u>In re Sealed</u>
3	<u>Case</u> .
4	
5	IV
6	Because plaintiffs have succeeded in alleging that they

7 are "aggrieved persons" under FISA, their request under § 1806(f) 8 is timely. Section 1806(f), discussed at some length in the 9 court's July 2 order (564 F Supp at 1131), is as follows: 10 Whenever a court or other authority is notified pursuant to subsection (c) or (d) of this section, or 11 whenever a motion is made pursuant to subsection (e) of this section, or whenever any motion or request is made 12 by an aggrieved person pursuant to any other statute or rule of the United States or any State before any court or other authority of the United States or any State to 13 discover or obtain applications or orders or other 14 materials relating to electronic surveillance or to discover, obtain, or suppress evidence or information 15 obtained or derived from electronic surveillance under this chapter, the United States district court or, 16 where the motion is made before another authority, the United States district court in the same district as 17 the authority, shall, notwithstanding any other law, if the Attorney General files an affidavit under oath that 18 disclosure or an adversary hearing would harm the national security of the United States, review in 19 camera and ex parte the application, order, and such other materials relating to the surveillance as may be 20 necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted. 21 In making this determination, the court may disclose to the aggrieved person, under appropriate security 22 procedures and protective orders, portions of the application, order, or other materials relating to the 23 surveillance only where such disclosure is necessary to make an accurate determination of the legality of the 24 surveillance. 25 Plaintiffs propose several approaches for the court to 26 allow plaintiffs to discover information about the legality of the 27 electronic surveillance under § 1806(f): 28  $\boldsymbol{\Lambda}$ 

Case/18::067-cv-01071999-VIRW Document 5377 Filied0011055220099 Filege220061225
1 (1) allow plaintiffs to examine a redacted version of
2 the Sealed Document that allows them to see anything 2 indicating whether defendants intercepted plaintiffs'
3 international telecommunications in March and April of 2004 and lacked a warrant to do so;
4 (2) impose a protective order prohibiting disclosure of any of the Sealed Document's contents;
5 (3) one or more of plaintiffs' counsel may obtain
6 security clearances prior to examining the Sealed Document (plaintiffs note that precedent exists for this 7 approach, pointing to attorneys at the Center for
8 Constitutional Rights who are involved in Guantanamo Bay 8 detention litigation and attaching the declaration of
one such attorney, Shayana Kadidal, describing the process of obtaining Top Secret/Sensitive Compartmented
Information ("TS/SCI") clearance for work on those cases (Doc #472-8/46-8)); and
11 (4) because they have already seen the Sealed Document,
12 plaintiffs' need would be satisfied by the court "simply 12 acknowledging [its] existence and permitting
[plaintiffs] to access portions of it and then reference13it — e g, in a sealed memorandum of points and
authorities — in our arguments on subsequent 14 proceedings to determine plaintiffs' standing.
15 Doc # 472/46 at 27.
16 In their opposition, defendants do not fully engage with
17 plaintiffs' motion, but rather seem to hold themselves aloof from
18 it:
19 [A]side from the fact that plaintiffs have failed to establish their standing to proceed as "aggrieved
20 persons" under the FISA, their motion should also be denied because Section 1806(f) does not apply in this
21 case — and should not be applied — for all the reasons previously set forth by the Government. Specifically,
22 the Government holds to its position that Section 1806(f) of the FISA does not preempt the state secrets
23 privilege, but applies solely where the Government has acknowledged the existence of surveillance in
24 proceedings where the lawfulness of evidence being used against someone is at issue. 25
<ul> <li>27 declarations with their opposition as seems to be called for by</li> <li>28 § 1806(f) upon the filing of a motion or request by an aggrieved</li> </ul>
20 3 1000(1) upon the fifting of a motion of request by an aggrieved
20

C	Casee\&::07-cv-0107199-VIRW Documment 537 Filided0011055220099 Fizegee221061225
1	person. Defendants, rather, assert that
2	The discretion to invoke Section 1806(f) belongs to the Attorney General, and under the present circumstances —
3	where there has been no final determination that those procedures apply in this case to overcome the
4	Government's successful assertion of privilege and where serious harm to national security is at stake — the
5	Attorney General has not done so. Section 1806(f) does not grant the Court jurisdiction to invoke those
6	procedures on its own to decide a claim or grant a moving party access to classified information, and any
7	such proceedings would raise would raise serious constitutional concerns.
8	constitutional concerns.
9	Id at 26-27, citing <u>Department of the Navy v Egan</u> , 484 US 518, 529
10	(1988) for the proposition that "the protection of national security
11	information lies within the discretion of the President under
12	Article II)." Of note, the court specifically rejected this very
13	reading of <u>Egan</u> in its July 2 order. See 564 F Supp 2d at 1121.
14	Defendants simply continue to insist that § 1806(f)
15	discovery may not be used to litigate the issue of standing; rather,
16	they argue, plaintiffs have failed to establish their "Article III
17	standing" and their case must now be dismissed. But defendants'
18	contention that plaintiffs must prove more than they have in order
19	to avail themselves of section 1806(f) conflicts with the express
20	primary purpose of in camera review under § 1806(f): "to determine
21	whether the surveillance of the aggrieved person was lawfully
22	authorized and conducted." § 1806(f).
23	In reply, plaintiffs call attention to the circular nature
24	of the government's position on their motion:
25	Do defendants mean to assert their theory of unfettered presidential power over matters of national security —
26	the very theory plaintiffs seek to challenge in this case — as a basis for disregarding this court's FISA
27	preemption ruling and defying the current access proceedings under section 1806(f)? So it seems.
28	
	21

Doc #515/53 at 17. So it seems to the court also.

It appears from defendants' response to plaintiffs' motion that defendants believe they can prevent the court from taking any action under 1806(f) by simply declining to act.

5 But the statute is more logically susceptible to another, 6 plainer reading: the occurrence of the action by the Attorney 7 General described in the clause beginning with "if" makes mandatory 8 on the district court (as signaled by the verb "shall") the in 9 camera/ex parte review provided for in the rest of the sentence. 10 The non-occurrence of the Attorney General's action does not necessarily stop the process in its tracks as defendants seem to 11 12 Rather, a more plausible reading is that it leaves the contend. 13 court free to order discovery of the materials or information sought by the "aggrieved person" in whatever manner it deems consistent 14 15 with section 1806(f)'s text and purpose. Nothing in the statute prohibits the court from exercising its discretion to conduct an in 16 17 camera/ex parte review following the plaintiff's motion and entering other orders appropriate to advance the litigation if the Attorney 18 19 General declines to act.

21

20

1

v

For the reasons stated herein, defendants' motion to dismiss or, in the alternative, for summary judgment (Doc #475/49), is DENIED. Plaintiffs' motion pursuant to 50 USC § 1806(f) is GRANTED (Doc #472/46).

The court has carefully considered the logistical problems and process concerns that attend considering classified evidence and issuing rulings based thereon. Measures necessary to

1 limit the disclosure of classified or other secret evidence must in 2 some manner restrict the participation of parties who do not 3 control the secret evidence and of the press and the public at The court's next steps will prioritize two interests: 4 large. 5 protecting classified evidence from disclosure and enabling plaintiffs to prosecute their action. Unfortunately, the important 6 7 interests of the press and the public in this case cannot be given 8 equal priority without compromising the other interests.

9 To be more specific, the court will review the Sealed 10 Document ex parte and in camera. The court will then issue an 11 order regarding whether plaintiffs may proceed — that is, whether 12 the Sealed Document establishes that plaintiffs were subject to electronic surveillance not authorized by FISA. As the court 13 understands its obligation with regard to classified materials, 14 15 only by placing and maintaining some or all of its future orders in this case under seal may the court avoid indirectly disclosing some 16 17 aspect of the Sealed Document's contents. Unless counsel for 18 plaintiffs are granted access to the court's rulings and, possibly, 19 to at least some of defendants' classified filings, however, the 20 entire remaining course of this litigation will be ex parte. This 21 outcome would deprive plaintiffs of due process to an extent 22 inconsistent with Congress's purpose in enacting FISA's sections 23 1806(f) and 1810. Accordingly, this order provides for members of 24 plaintiffs' litigation team to obtain the security clearances 25 necessary to be able to litigate the case, including, but not 26 limited to, reading and responding to the court's future orders.

27Given the difficulties attendant to the use of classified28material in litigation, it is timely at this juncture for

1 defendants to review their classified submissions to date in this 2 litigation and to determine whether the Sealed Document and/or any 3 of defendants' classified submissions may now be declassified. Accordingly, the court now directs defendants to undertake such a 4 5 review.

The next steps in this case will be as follows:

Within fourteen (14) days of the date of this order, 1. defendants shall arrange for the court security officer/security specialist assigned to this case in the Litigation Security Section of the United States Department of Justice to make the Sealed 11 Document available for the court's in camera review. If the Sealed 12 Document has been included in any previous classified filing in this matter, defendants shall so indicate in a letter to the court. 13

14 Defendants shall arrange for Jon B Eisenberg, lead 2. 15 attorney for plaintiffs herein and up to two additional members of plaintiffs' litigation team to apply for TS/SCI clearance and shall 16 17 expedite the processing of such clearances so as to complete them 18 no later than Friday, February 13, 2009. Defendants shall 19 authorize the court security officer/security specialist referred 20 to in paragraph 1 to keep the court apprised of the status of these 21 Failure to comply fully and in good faith with the clearances. 22 requirements of this paragraph will result in an order to show 23 cause re: sanctions.

24 Defendants shall review the Sealed Document and their 3. classified submissions to date in this litigation and determine 25 26 whether the Sealed Document and/or any of defendants' classified 27 submissions may be declassified, take all necessary steps to 28 declassify those that they have determined may be declassified and,

6

7

8

9

10

no later than forty-five (45) days from the date of this order,
 serve and file a report of the outcome of that review.

3 The parties shall appear for a further case 4. 4 management conference on a date to be determined by the deputy 5 clerk within the month of January 2009. Counsel should be prepared 6 to discuss adjudication of any and all issues that may be conducted 7 without resort to classified information, as well as those issues 8 that may require such information. Counsel shall, after 9 conferring, submit brief statements of their respective plans or a 10 joint plan, if they agree to one.

IT IS SO ORDERED.

VAUGHN R WALKER United States District Chief Judge

For the Northern District of California **United States District Court** 

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27