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

ORDER

This order pertains to:

Al-Haramain Islamic Foundation et al v Bush et al (C-07-0109 VRW),

/

The court of appeals has remanded the above case for this court "to consider whether FISA preempts the state secrets privilege and for any proceedings collateral to that determination." Al-Haramain Islamic Foundation, Inc v Bush, 507 F3d 1190, 1206 (9th Cir 2007).

Plaintiffs' complaint alleges six causes of action of which the first is under the Foreign Intelligence Surveillance Act, 50 USC §§ 1801-71 ("FISA"). In that claim, plaintiffs allege in pertinent part:

> **Defendants' engagement in electronic surveillance to monitor conversations between and among plaintiffs as targeted persons without obtaining prior court authorization, and defendants' subsequent use of the information obtained against plaintiffs, is in violation of the civil and criminal provisions of**

> **FISA. As a result, all evidence obtained by this illegal surveillance must be suppressed pursuant to 50 USC § 1806(g). Further, plaintiffs are entitled to liquidated and punitive damages pursuant to 50 USC § 1810.**

Complaint, Al-Haramain Islamic Foundation, Inc v Bush, No C 06-0274 KI Doc # 1 ¶ 27, United States District Court for the District of Oregon, filed February 28, 2006.

Plaintiffs' other causes of action are for alleged violations of the "separation of powers" principle in the Constitution, the First, Fourth and Sixth amendments and the International Covenant on Civil and Political Rights. But it is to plaintiffs' FISA claims that the parties have directed their arguments and the court of appeals its attention. All of plaintiffs' claims would appear to depend on FISA. This order, therefore, devotes itself exclusively to FISA and the question posed by the court of appeals remand.

For the reasons stated herein, the court has determined that: (1) FISA preempts the state secrets privilege in connection with electronic surveillance for intelligence purposes and would appear to displace the state secrets privilege for purposes of plaintiffs' claims; and (2) FISA nonetheless does not appear to provide plaintiffs a viable remedy unless they can show that they are "aggrieved persons" within the meaning of FISA. The lack of precedents interpreting the remedial provisions of FISA, the failure of the parties to consider the import of FISA preemption and the undeveloped factual record in this case warrant allowing plaintiffs to attempt to make that showing and, therefore, support dismissal of the FISA claim with leave to amend.

****

I

Plaintiffs are the Al-Haramain Islamic Foundation, Inc, an Oregon non-profit corporation, and two of its individual attorneys, Wendell Belew and Asim Ghafoor, both United States citizens ("plaintiffs"). Plaintiffs brought suit in the United States District Court for the District of Oregon against "George W Bush, President of the United States, National Security Agency, Keith B Alexander, its Director, Office of Foreign Assets Control, an office of the United States Treasury, Robert W Werner, its Director, Federal Bureau of Investigation, Robert S Mueller, III, its Director" ("defendants"). Complaint at 1.

Along with their complaint, plaintiffs filed under seal a copy of a classified document that had inadvertently been disclosed by defendant Office of Foreign Assets Control ("OFAC") to counsel for Al-Haramain as part of a production of unclassified documents relating to Al-Haramain's potential status as a "specially designated global terrorist." Al-Haramain Islamic Foundation, Inc v Bush, 451 F Supp 2d 1215, 1218 (D Or 2006).[1] This document, which has proven central to all phases of this litigation including the issues now before this court, will be referred to herein as the "Sealed Document."

The complaint alleges that the National Security Agency ("NSA") conducted warrantless electronic surveillance of communications between a director or directors of Al-Haramain and

[1] On June 19, 2008, the United States Department of the Treasury designated "the entirety" of the Al-Haramain Islamic Foundation including its headquarters in Saudi Arabia, having previously designated branch offices in thirteen individual countries, including the United States. See http://www.treasury.gov/press/releases/hp1043.htm.

the two attorney plaintiffs without regard to the procedures required by FISA, that the NSA turned over logs from this surveillance to OFAC and that OFAC then consequently froze Al-Haramain's assets. Id.

The Oregon district court entertained motions by the Oregonian Publishing Company to intervene in the suit and unseal records, by plaintiffs to compel discovery of information about the electronic surveillance of plaintiffs and regarding the reasons for classifying the Sealed Document and by defendants to prevent plaintiffs' access to the Sealed Document and to dismiss or, in the alternative, for summary judgment based on the state secrets privilege.

On September 7, 2006, the Oregon district court issued a lengthy opinion and order. Several points in that order remain salient to the matter now before this court. The court held that "plaintiffs need some information in the Sealed Document to establish their standing and a prima facie case, and they have no other available source for this information." Id at 1221. It also held that given defendants' many public acknowledgments of the warrantless electronic surveillance program beginning in 2005, the program was not a secret. Id at 1221-23. It rejected defendants' contention that litigation concerning the program would necessarily compromise national security and held that, contrary to defendants' contention, "the very subject matter of the case" was not a state secret. It ordered plaintiffs to deliver to the court all copies of the Sealed Document in their possession or under their control, to be deposited in the sealed compartmentalized information facility ("SCIF") provided by the Portland FBI office for the

storage of classified documents. Id at 1229. It denied without prejudice plaintiffs' request for discovery and denied the Oregonian's motion to unseal records. Id at 1232.

The Oregon district court ruled that there was "no reasonable danger that the national security would be harmed if it is confirmed or denied that plaintiffs were subject to surveillance, but only as to the surveillance event or events disclosed in the Sealed Document" while also ruling that "disclosing whether plaintiffs were subject to any other surveillance efforts could harm the national security." Id at 1224 (emphasis added). On the rationale that plaintiffs should be allowed to proceed based on the surveillance already disclosed to them, substantiated by evidence in a form yet to be determined, the court denied defendants' motion to dismiss: "plaintiffs should have an opportunity to establish standing and make a prima facie case, even if they must do so in camera." Id at 1226-27.

The Oregon district court declined to reach one further issue presented to it by the parties——the issue this court is charged to decide on remand from the court of appeals:

> Plaintiffs argue * * * that FISA preempts the state secrets privilege. Specifically, plaintiffs argue that FISA vests the courts with control over materials relating to electronic surveillance, subject to "appropriate security procedures and protective orders." 50 USC §1806(f). As a result, plaintiffs contend that Section 1806(f) renders the state secrets privilege superfluous in FISA litigation.

Id at 1229.

The Oregon district court summarized defendants' argument to be that section 1806(f) only benefits the government——that it exists, in essence, for the sole purpose of providing for in camera

review of documents and information the government intends to use against a criminal defendant. The Oregon district court quoted section 1810, FISA's civil liability provision, together with FISA's definition of an "aggrieved person" entitled to sue under section 1810 (see infra Part III) and observed: "[t]o accept the government's argument that Section 1806(f) is only applicable when the government intends to use information against a party would nullify FISA's private remedy and would be contrary to the plain language of Section 1806(f)." Id at 1231 (emphasis added).

Concluding that "[t]he question becomes then whether Section 1806(f) preempts the state secrets privilege," the Oregon district court wrote, "I decline to reach this very difficult question at this time, which involves whether Congress preempted what the government asserts is a constitutionally-based privilege." Id. The Oregon district court certified its other rulings for immediate appeal. Defendants appealed and, during the pendency of the appeal, this case was reassigned by the Judicial Panel on Multidistrict Litigation ("MDL") to the undersigned.

The court of appeals granted interlocutory review and consolidated the appeal in this matter with the interlocutory appeal from an order by the undersigned concerning the state secrets privilege and related issues in Hepting v AT&T Corp, 439 F Supp 2d 974 (N D Cal 2006). The cases were argued on the same day before the same panel, but the court of appeals later determined that "the claimed facts and circumstances of each case are distinct" and entered an order concurrently with the opinion in the instant matter stating that "the cases are no longer consolidated for any purpose." 507 F3d at 1196 n 3. The court of appeals

subsequently issued an order withdrawing the submission of the Hepting appeal; that matter remains on appeal. Order, Hepting v AT&T Corporation, Inc, No 06-17137 Doc #128, United States Court of Appeals for the Ninth Circuit, filed November 16, 2007.

In its opinion in this case, the court of appeals determined that review of a district court's rulings on the state secrets privilege should be de novo, having previously only "intimated" as much. 507 F3d at 1196. After considering the history of the state secrets privilege, the court of appeals considered three contentions by the government on appeal: (1) the very subject matter of the litigation is a state secret; (2) Al-Haramain cannot establish standing to bring suit, absent the Sealed Document; and (3) Al-Haramain cannot establish a prima facie case, and the government cannot defend against Al-Haramain's assertions, without resorting to state secrets. In a footnote, the court of appeals observed that the third issue had not been addressed by the district court. 507 F3d at 1197 & n 4.

As to the first issue, the court of appeals made note of the government's extensive, intentional public disclosures by President George W Bush, Attorney General Alberto Gonzales and especially General Michael V Hayden, which had "provided to the American public a wealth of information about the [Terrorist Surveillance Program]," and declined to follow either Kasza v Browner, 133 F3d 1159 (9th Cir 1998) or El-Masri v United States, 479 F3d 296 (4th Cir 2007), both cases in which dismissals based on the state secrets privilege were affirmed on appeal. The court held that while Al-Haramain's case involved privileged information, "that fact alone does not render the very subject matter of the

action a state secret" and affirmed the district court's denial of dismissal on that basis. 507 F3d at 1201.

Before turning to the second issue on appeal, the court of appeals next considered whether the state secrets privilege had been properly invoked and determined that it had. Based on that determination, the court of appeals concluded that Al-Haramain's "showing of necessity" or "admittedly substantial need for the document to establish its case," United States v Reynolds, 345 US 1, 10 (1953), required an in camera review of the Sealed Document. 507 F3d at 1203. After describing in general terms the nature of the in camera review, the court wrote: "We are satisfied that the basis for the privilege is exceptionally well documented" and that disclosure of "information concerning the Sealed Document and the means, sources and methods of intelligence gathering in the context of this case would undermine the government's intelligence capabilities and compromise national security." 507 F3d at 1204. The court of appeals then held that the Oregon district court's compromise allowing plaintiffs to submit sealed affidavits attesting to the contents of the document from their memories was "contrary to established Supreme Court precedent"—— specifically Reynolds, 345 US at 11——and wrote that "the state secrets privilege * * * does not lend itself to a compromise solution in this case." Id.

Regarding use of the Sealed Document in this litigation, the court of appeals held: "The Sealed Document, its contents, and any individuals' memories of its contents, even well-reasoned speculation as to its contents, are completely barred from further disclosure in this litigation by the common law state secrets privilege." Id.

Having thus dealt with the first issue, the court of appeals turned to the government's second issue on appeal——Al-Haramain's standing——and held that plaintiffs could not establish standing to proceed with their lawsuit without the Sealed Document because they could not establish a "concrete and particularized" injury-in-fact under the principles of Lujan v Defenders of Wildlife, 504 US 555 (1992): "Al-Haramain cannot establish that it has standing, and its claims must be dismissed, unless FISA preempts the state secrets privilege." 507 F3d 1205.

Citing Singleton v Wulff, 428 US 106 (1976), that a court of appeals should not ordinarily consider an issue not ruled on in the district court, the court of appeals declined to decide whether FISA preempts the state secrets privilege. Instead, writing that "the FISA issue remains central to Al-Haramain's ability to proceed with this lawsuit," it remanded the case to this court to consider that question "and for any proceedings collateral to that determination." 507 F3d at 1206. The court of appeals did not consider the consequences of FISA preempting the state secrets privilege and the implications of such a determination for possible use in this litigation of the Sealed Document.

In accordance with orders entered at a status conference in this matter on February 7, 2008, defendants filed a second motion to dismiss plaintiffs' claims on the grounds that FISA does not preempt the state secrets privilege and that plaintiffs lack standing to seek prospective relief and are barred from seeking relief under FISA by the doctrine of sovereign immunity. Doc

\\

\\

#432/17.[2] Plaintiffs filed an opposition (Doc #435/20) and the court accepted two amicus briefs, one by plaintiffs in other MDL cases and the other by certain telecommunications defendants in the MDL cases (Doc ##440/23 & 442/25).

II

A

The enactment of FISA was the fruition of a period of intense public and Congressional interest in the problem of unchecked domestic surveillance by the executive branch. In 1975, Congress formed the Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities known as the "Church Committee" for its chairman, Senator Frank Church, to investigate alleged intelligence-gathering abuses in the domestic sphere by the various executive branch agencies with intelligence-gathering authority. The Church Committee's two-volume final report was transmitted to Congress in 1976; the following passage from among the report's conclusions and recommendations illustrates the tone and substance of the findings:

> Our findings and the detailed reports which supplement this volume set forth a massive record of intelligence abuses over the years. Through the use of a vast network of informants, and through the uncontrolled or illegal use of intrusive techniques——ranging from simple theft to sophisticated electronic surveillance——the Government has collected, and then used improperly, huge amounts of information about the private lives, political beliefs and associations of numerous Americans.

[2] Citations to documents in the docket of this case will be cited both to the MDL docket (No M 06-1791 VRW) and to the individual docket (No C 07-0109) in the following format: Doc #xxx/yy.

Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities ("Church Committee Report") Book II: Intelligence Activities and the Rights of Americans, S Rep No 94-755, 290 (1976).

The Church Committee Report further concluded that "intelligence activities have undermined the constitutional rights of citizens and that they have done so primarily because checks and balances designed by the framers of the Constitution to assure accountability have not been applied." Id at 289. The Church Committee Report set the stage for Congress to begin the effort to enact comprehensive legislation to address the intelligence-related abuses identified therein. That effort began in the very next Congress.

In 1978, after the introduction of several competing bills and extensive deliberation and debate, Congress enacted FISA. To summarize FISA's provisions in a brief and general manner, FISA set out in detail roles for all three branches of government, providing judicial and congressional oversight of the covert surveillance activities by the executive branch combined with measures to safeguard secrecy necessary to protect national security. FISA set out procedures by which the executive branch could undertake electronic surveillance and physical searches for foreign intelligence purposes in the domestic sphere. Any application for electronic surveillance was required, among other things, to establish probable cause justifying the surveillance, describe the information being sought and aver that the information could not be obtained through normal investigative techniques. 50 USC § 1804(a).

\\

FISA also provided for the creation of two courts staffed by federal judges to conduct sealed proceedings to consider requests by the government for warrants to conduct foreign intelligence surveillance. 50 USC §§ 1803(a),(b). The Foreign Intelligence Surveillance Court ("FISC") was established to consider applications in the first instance, with the Court of Review reviewing denials of applications by the FISC and the Supreme Court acting as the final appellate court. Id. FISA allowed the United States attorney general to authorize electronic surveillances in emergency situations without FISC approval if the appropriate judge was informed and an application made within twenty-four hours after authorization. 50 USC §§ 1802, 1805(f).

FISA provided for continuing oversight of the government's foreign intelligence surveillance activities by Congress, requiring regular, highly detailed reports to Congress of all actions taken under FISA. E g, 50 USC §§ 1808, 1826. The reporting requirements are discussed in more detail in Part III A below.

Of special relevance to the court's present inquiry, Congress included in the FISA bill a declaration that the FISA regime, together with **the Omnibus Crime Control and Safe Streets Act of 1968 codified at chapter 119 of Title 18 of the United States Code, 18 USC §§ 2510-22** ("Title III"), were to be the "exclusive means" by which domestic electronic surveillance for national security purposes could be conducted:

> procedures in this chapter or chapter 121 and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance, as defined in section 101 of such Act, and the interception of domestic wire, oral, and electronic communications may be conducted.

18 USC § 2511(2)(f). This provision and its legislative history left no doubt that Congress intended to displace entirely the various warrantless wiretapping and surveillance programs undertaken by the executive branch and to leave no room for the president to undertake warrantless surveillance in the domestic sphere in the future.

The Report of the Senate Select Committee on Intelligence stated that the FISA bill's "exclusive means" statement "puts to rest the notion that Congress recognizes an inherent Presidential power to conduct such surveillances in the United States outside of the procedures contained in chapters 119 and 120." Foreign Intelligence Surveillance Act, S Rep No 95-701, 95th Cong 2d Sess 71, reprinted in 1978 USCCAN 3973, 4040. That report cited Congress's authority over FISA's subject matter in Article I section 8 of the Constitution and the power to "make all laws which shall be necessary and proper for carrying into execution the foregoing powers." US Const cl 1, 18. The report also both discussed Justice Jackson's concurring opinion in Youngstown Sheet and Tube Co v Sawyer, 343 US 579, 635 (1952) and included the following passage from the opinion:

> When the President takes measures incompatible with the expressed or implied will of Congress, his power is at its lowest ebb, for then he can rely only upon his own constitutional powers minus any constitutional power of Congress over the matter.

See also Foreign Intelligence Surveillance Act, H Conf Rep No 95-1720, 95th Cong 2d Sess 35, reprinted in 1978 USCCAN 4048, 4064. ("The intent of the conferees is to apply the standard set forth in Justice Jackson's concurring opinion in [Youngstown Sheet & Tube].")

A lesser-known provision of FISA also expressly limited

presidential power to conduct foreign intelligence surveillance by repealing 18 USC section 2511(3) which had provided:

> Nothing in this chapter * * * shall limit the constitutional power of the President to take such measures as he deems necessary to protect the nation against actual or potential attack * * * or to protect national security against foreign intelligence activities. * * * The contents of any wire or oral communication intercepted by authority of the President in the exercise of the foregoing powers may be received in evidence in any trial hearing [sic], or other proceeding only where such interception was reasonable, and shall not be otherwise used or disclosed except as is necessary to implement that power.

18 USC § 2511(3)(1976). The Report of the Senate Select Committee on Intelligence explained that the repeal of this section "eliminat[ed] any congressional recognition or suggestion of inherent Presidential power with respect to electronic surveillance." S Rep 95-701, 72.

In the floor debate on Senate Bill 1566, Senator Gaylord Nelson related the history of the Senate's efforts to enact a foreign intelligence surveillance law to curb the abuses reported by the Church Committee; he noted that a "principal issue" with prior, unsuccessful legislative proposals was the reservation or reference to "inherent Presidential power," but that Senate Bill 1566 had no such reservation or reference: "Once enacted, it would represent the sole authority for national security electronic surveillance in the United States." Foreign Intelligence Surveillance Act, S 1566, 95th Cong, 2d Sess, in 124 Cong Rec S 10903 (April 30, 2978). Senator Nelson further stated: "Along with the existing statute dealing with criminal wiretaps, this legislation blankets the field. If enacted, the threat of warrantless electronic surveillance will be laid to rest." Id.

B

"Preemption" usually refers to Congress asserting its authority under the Supremacy Clause to override state law that interferes with federal interests. In the present context, "preemption" refers to Congress overriding or replacing the interstitial lawmaking that judges create through federal common law. In Milwaukee v Illinois, 451 US 304, 314 (1980) the Supreme Court explained the latter type of preemption: "Federal common law is a 'necessary expedient' and when Congress addresses a question previously governed by a decision rested on federal common law the need for such an unusual exercise of lawmaking by federal courts disappears." The Court further explained that federal courts need not find a "clear and manifest purpose" to replace or displace federal common law as would be required for a determination that Congress had pre-empted state law because there are no corresponding concerns for "our embracing federal system, including the principle of diffusion of power * * * as a promoter of democracy." Id at 316-17. On the contrary, the Court noted that federal courts are not general common-law courts and do not possess "a general power to develop and apply their own rules of decision." Id at 312, citing Erie R Co v Tompkins, 304 US 64, 78 (1934). Federal common law applies "[u]ntil the field has been made the subject of comprehensive legislation." 451 US at 314.

In Milwaukee v Illinois, the Court held that the 1972 amendments to the Federal Water Pollution Control Act preempted the application of the common law of nuisance by federal courts in disputes over water pollution. In so holding, the Court looked to the legislative history, making special note of remarks by the Act's

sponsors, in determining that Congress's purpose was to establish an "all-encompassing program of water pollution regulation" 451 US at 318. The Court noted that "[n]o Congressman's remarks were complete without reference to the 'comprehensive' nature of the Amendments." Id. "The establishment of such a self-consciously comprehensive program by Congress * * * strongly suggests that there was no room for courts to attempt to improve on that program with federal common law." Id at 319.

Both the plain text and the legislative history make clear that Congress intended FISA to "occupy the field through the establishment of a comprehensive regulatory program supervised by an expert administrative agency." Id at 317. Congress through FISA established a comprehensive, detailed program to regulate foreign intelligence surveillance in the domestic context. The establishment of the specialized FISA courts specifically dedicated to considering requests for foreign intelligence surveillance by the executive branch paralleled the "expert administrative agency" referred to with approval in Milwaukee v Illinois.

The present preemption analysis departs from that in Milwaukee v Illinois with respect to the scope and nature of what is being displaced. The court is charged with determining whether FISA preempts or displaces not a common-law set of rules for conducting foreign intelligence surveillance, but rather a privilege asserted by the government to avoid public and judicial scrutiny of its activities related to national security. In this case, those activities include foreign intelligence surveillance, the subject matter that Congress through FISA sought comprehensively to regulate. This imperfect overlap between the preempting statute and

the common-law rule being preempted does not, however, create serious problems with finding the state secrets privilege preempted or displaced by FISA in the context of matters within FISA's purview. FISA does not preempt the state secrets privilege as to matters that are not within FISA's purview; for such matters, the lack of comprehensive federal legislation leaves an appropriate role for this judge-made federal common law privilege.

"The state secrets privilege is a common law evidentiary privilege that protects information from discovery when disclosure would be inimical to the national security. [It] has its modern roots in United States v Reynolds." In re United States, 872 F2d 472, 474 (DC Cir 1989). "The state secrets privilege is a common law evidentiary privilege that permits the government to bar the disclosure of information if 'there is a reasonable danger' that disclosure will 'expose military matters which, in the interest of national security, should not be divulged.'" Al-Haramain Islamic Foundation v Bush, 507 F3d at 1196, citing Reynolds, 345 US at 10. The undersigned discussed the history and operation of the state secrets privilege at some length in Hepting v AT&T Corp, 439 F Supp 2d 974 at 980-85 (N D Cal 2006).

Reynolds largely demarcated the state secrets privilege as it is understood today, that is: it belongs to the government; it must be properly invoked by means of a "formal claim of privilege, lodged by the head of the department which has control over the matter" after "actual consideration"; the court must then "determine whether the circumstances are appropriate for the claim of privilege, and yet do so without forcing a disclosure of the very thing the privilege is designed to protect"; the precise nature,

extent and manner of this inquiry depends in part on the extent of a party's need for the information sought tested against the strength of the government's claim of privilege; and in camera review might be appropriate in some cases, but not all. "When compulsion of the evidence will expose military matters which, in the interest of national security, should not be divulged, * * * the court should not jeopardize the security which the privilege is meant to protect by insisting upon an examination of the evidence, even by the judge alone, in chambers." 345 US at 7-10.

Plaintiffs argue that the in camera procedure described in FISA's section 1806(f) applies to preempt the protocol described in Reynolds in this case. Doc # 435/20 at 11-14. The court agrees. Section 1806(f), which is quoted in full and discussed at greater length in Part III B below, provides that in cases in federal courts in which "aggrieved persons" seek to discover materials relating to, or information derived from, electronic surveillance, the United States attorney general may file "an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States." In that event, the court "shall" conduct an in camera, ex parte review of such materials relating to the surveillance "as may be necessary to determine whether the surveillance * * * was lawfully authorized and conducted." The procedure described in section 1806(f), while not identical to the procedure described in Reynolds, has important characteristics in common with it——enough, certainly, to establish that it preempts the state secrets privilege as to matters to which it relates. Section 1806(f) is Congress's specific and detailed prescription for how courts should handle claims by the government that the disclosure of

material relating to or derived from electronic surveillance would harm national security; it leaves no room in a case to which section 1806(f) applies for a Reynolds-type process. Moreover, its similarities are striking enough to suggest that section 1806(f), which addresses a range of circumstances in which information derived from electronic surveillance might become relevant to judicial proceedings, is in effect a codification of the state secrets privilege for purposes of relevant cases under FISA, as modified to reflect Congress's precise directive to the federal courts for the handling of materials and information with purported national security implications. In either event, the Reynolds protocol has no role where section 1806(f) applies. For that reason, the court of appeals' reliance on Reynolds in connection with the Sealed Document, while perhaps instructive, would not appear to govern the treatment of that document under FISA.

The legislative history, moreover, buttresses the court's reading of the statutory text as intending that FISA replace judge-made federal common law rules:

> [T]he development of the law regulating electronic surveillance for national security purposes has been uneven and inconclusive. This is to be expected where the development is left to the judicial branch in an area where cases do not regularly come before it. Moreover, the development of standards and restrictions by the judiciary with respect to electronic surveillance for foreign intelligence purposes accomplished through case law threatens both civil liberties and the national security because that development occurs generally in ignorance of the facts, circumstances, and techniques of foreign intelligence electronic surveillance not present in the particular case before the court. * * * [T]he tiny window to this area which a particular case affords provides inadequate light by which judges may be relied upon to develop case law which adequately balances the rights of privacy and national security.

Foreign Intelligence Surveillance Act of 1978, HR Rep No 95-1283 Part I at 21. This legislative history is evidence of Congressional intent that FISA should displace federal common law rules such as the state secrets privilege with regard to matters within FISA's purview.

Defendants advance essentially three points in support of their contention that "nothing in FISA indicates any intention by Congress * * * to abrogate the state secrets privilege" in the case of intelligence-driven electronic surveillance. Doc #432/17 at 13. First, defendants argue that the privilege derives, not only from the common law, but also from the president's Article II powers, so that a "clear expression" of congressional intent is required to abrogate that privilege; furthermore, abrogation would raise fundamental constitutional problems which should be avoided. Doc #432/17 at 13-14. Second, defendants note the common law origins of the state secrets privilege and advert to the principle that abrogation of common law requires a "clear and direct" legislative expression of intent, which they contend is absent. Id at 14-15. Finally, defendants contend that section 1806(f) serves a fundamentally different purpose from the state secrets privilege and that the former cannot therefore "preempt" the latter because section 1806(f) governs disclosure by the government of intelligence derived from electronic surveillance whereas the state secrets privilege is fundamentally a rule of non-disclosure. Id at 15-22. The court disagrees with all three of these contentions, the second and third of which have been fully addressed in the paragraphs above.

\\

The weakness of defendants' first argument——that the Constitution grants the executive branch the power to control the state secrets privilege——is evident in the authorities they marshal for it. Defendants rely on United States v Nixon, 418 US 683 (1974), in which the Supreme Court rejected President Nixon's efforts to quash subpoenas under Federal Rule of Criminal Procedure 17(c) seeking tape recordings and documents pertaining to the Watergate break-in and ensuing events. The Court rejected the president's "undifferentiated claim of public interest in the confidentiality of [White House] conversations" between the president and his advisors, contrasting the need for confidentiality of these conversations with "a claim of need to protect military, diplomatic or sensitive national security secrets." Id at 706. In the course of making this comparison, the Court observed that privileges against forced disclosure find their sources in the Constitution, statutes or common law. At bottom, however, Nixon stands for the proposition that in the case of a common law privilege such as that asserted by President Nixon, it is the judiciary that defines the metes and bounds of that privilege and even the confidential communications of the president must yield to the needs of the criminal justice system. This hardly counts as authority that the president's duties under Article II create a shield against disclosure.

Even the Court's comparative weighing of the imperatives of confidentiality for "undifferentiated" presidential discussions and "military, diplomatic or sensitive national security secrets" affords defendants little help in this case. Department of the Navy v Egan, 484 US 518 (1988), upon which defendants rely, confirms that

power over national security information does not rest solely with the president. Egan recognized the president's constitutional power to "control access to information bearing on national security," stating that this power "falls on the President as head of the Executive Branch and as Commander in Chief" and "exists quite apart from any explicit congressional grant." Id at 527. But Egan also discussed the other side of the coin, stating that "unless Congress specifically has provided otherwise, courts traditionally have been reluctant to intrude upon the authority of the Executive in military and national security affairs." Id at 530 (emphasis added). Egan recognizes that the authority to protect national security information is neither exclusive nor absolute in the executive branch. When Congress acts to contravene the president's authority, federal courts must give effect to what Congress has required. Egan's formulation is, therefore, a specific application of Justice Jackson's more general statement in Youngstown Sheet & Tube.

It is not entirely clear whether defendants acknowledge Congress's authority to enact FISA as the exclusive means by which the executive branch may undertake foreign intelligence surveillance in the domestic context. While their papers do not explicitly assert otherwise, defendants' attorney in this matter stated in open court during the hearing herein held on April 23, 2008 that, while he conceded that "Congress sought to take over the field" of foreign intelligence surveillance (Doc #452 at 29:2-3), whether the president actually had constitutional authority under Article II to order such surveillance in disregard of FISA remained an open question: "[D]oes the president have constitutional authority under Article II to authorize foreign intelligence surveillance? Several

courts said that he did. Congress passed the FISA, and the issue has never really been resolved. That goes to the issue of the authority to authorize surveillance." Id at 33:7-12. Counsel repeatedly asserted that this issue was entirely separate from the preemption inquiry relevant to the state secrets privilege and urged the court not to "conflate" the two inquiries. E g, id at 32:8-10.

To the contrary, the court believes that the two areas of executive branch activity pertaining to foreign intelligence surveillance are not distinct for purposes of this analysis as defendants' counsel asserts. Congress appears clearly to have intended to——and did——establish the exclusive means for foreign intelligence surveillance activities to be conducted. Whatever power the executive may otherwise have had in this regard, FISA limits the power of the executive branch to conduct such activities and it limits the executive branch's authority to assert the state secrets privilege in response to challenges to the legality of its foreign intelligence surveillance activities.

Of note, many Congressional enactments regulate the use of classified materials by the executive branch, putting FISA in good company. Title 50 chapter 15 of the United States Code relates to national security generally and national security information in particular. Some of its provisions restrict disclosure and impose minimum security requirements on the executive branch. Fifty USC section 435 requires the president to "establish procedures to govern access to classified information," such as background checks. Others authorize disclosure. Fifty USC section 403-5d, part of the

USA PATRIOT Act[3], permits federal law enforcement officials to share foreign intelligence information obtained as part of a criminal investigation. Other provisions allocate control of classified material among executive branch agencies. For instance, 50 USC section 435a(d) gives the director of the Central Intelligence Agency the power to control the State Department's use of classified information. Congress elsewhere requires the executive branch to disclose national security information to Congressional intelligence committees. 50 USC §§ 413(a), 413b(c). Congress left the executive branch no "authority to withhold information from the intelligence committees on the grounds that providing the information to the intelligence committees would constitute the unauthorized disclosure of classified information or information relating to intelligence sources and methods." 50 USC § 413(e). See also 50 USC § 425 ("Nothing" in subchapter IV, which pertains to "Protection of Certain National Security Information," "may be construed as authority to withhold information from the Congress or from a committee of either House of Congress.") And 50 USC section 413(b) requires that "[t]he President shall ensure that any illegal intelligence activity is reported promptly to the intelligence committees * * *." Congressional regulation of the use of classified information by the executive branch through FISA and other statutes is therefore well-established.

As part of their argument that the state secrets privilege has a constitutional basis in Article II, defendants contend that a

---

[3] **Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism ("USA PATRIOT") Act of 2001, Pub L No 107-56, § 215, 115 Stat 287, amended by USA Patriot Improvement and Reauthorization Act of 2005, Pub L 109-178, 120 Stat 282 (2006).**

"clear statement of congressional intent" to abrogate the privilege is required, citing Franklin v Massachusetts, 505 US 788, 800-01 (1992). Franklin held that the office of the president was not an executive "agency" whose actions were subject to judicial review under the Administrative Procedures Act. The APA broadly described its scope to include "each authority of the Government of the United States" except Congress, the courts, the governments of United States territories and the government of Washington, DC. The Court nonetheless held that, when the APA did not explicitly include the president and the legislative history did not suggest that Congress intended for courts to review the president's actions under the APA, the APA's "textual silence" was insufficient to infer that Congress intended to subject the president to lawsuits under the APA: "We would require an express statement by Congress before assuming it intended the President's performance of his statutory duties to be reviewed for abuse of discretion." See also Nixon v Fitzgerald, 457 US 731, 748, n27 (1982) (Court would require an explicit statement by Congress before assuming Congress had created a damages action against the president)." Franklin, 505 US at 800-01.

Franklin is readily distinguishable. The impetus for the enactment of FISA was Congressional concern about warrantless wiretapping of United States citizens conducted under a justification of inherent presidential authority under Article II. Congress squarely challenged and explicitly sought to prohibit warrantless wiretapping by the executive branch by means of FISA, as FISA's legislative history amply documented. This was a different situation from Franklin, in which the Court required certainty about Congressional intent to regulate the office of the

president that was absent on the record before it.

In the case of FISA, Congress attempted not only to put a stop to warrantless wiretapping by the executive branch but also to establish checks and balances involving other branches of government in anticipation of efforts by future administrations to undertake warrantless surveillance in some other manner:

> In the past several years, abuses of domestic national security surveillances have been disclosed. This evidence alone should demonstrate the inappropriateness of relying solely on executive branch discretion to safeguard civil liberties. This committee is well aware of the substantial safeguards respecting foreign intelligence electronic surveillance currently embodied in classified Attorney General procedures, but this committee is also aware that over the past thirty years there have been significant changes in internal executive branch procedures, and there is ample precedent for later administrations or even the same administration loosening previous standards.

H R Rep No 95-1283(I) at 21. Given the possibility that the executive branch might again engage in warrantless surveillance and then assert national security secrecy in order to mask its conduct, Congress intended for the executive branch to relinquish its near-total control over whether the fact of unlawful surveillance could be protected as a secret.

Reynolds itself, holding that the state secrets privilege is part of the federal common law, leaves little room for defendants' argument that the state secrets privilege is actually rooted in the constitution. Reynolds stated that the state secrets privilege was "well-established in the law of evidence." 345 US at 6-7. At the time, Congress had not yet approved the Federal Rules of Evidence, and therefore the only "law of evidence" to apply in federal court was an amalgam of common law, local practice and

statutory provisions with indefinite contours. John Henry Wigmore (revised by Peter Tillers), I Evidence §6.1 at 384-85 (Little, Brown & Co 1983). The Court declined to address the constitutional question whether Congress could limit executive branch authority to withhold sensitive documents, but merely interpreted and applied federal common law. See Reynolds, 345 US at 6 & n9.

Defendants' attempt to establish a strict dichotomy between federal common law and constitutional interpretation is, moreover, misconceived because all rules of federal common law have some grounding in the Constitution. "Federal common law implements the federal Constitution and statutes, and is conditioned by them. Within these limits, federal courts are free to apply the traditional common-law technique of decision and to draw upon all the sources of the common law in cases such as the present." D'Oench, Duhme & Co v FDIC, 315 US 447, 472 (1942) (Jackson concurring). The rules of federal common law on money and banking, for instance, all derive from the Constitution. See Clearfield Trust Co v United States, 318 US 363, 366 (1943) (in disbursements of funds and payment of debts, United States exercises a constitutional function or power). The federal common law pertaining to tort suits brought by United States soldiers against private tortfeasors flows from Congress's powers under Article I section 8. United States v Standard Oil Co, 332 US 301, 306 n7 (1947). Accordingly, all rules of federal common law perform a function of constitutional significance.

In the specific context of the state secrets privilege, it would be unremarkable for the privilege to have a constitutional "core" or constitutional "overtones." See Robert M Chesney, State

Secrets and the Limits of National Security Litigation, 75 George Wash L Rev 1249, 1309-10 (2007). Article II might be nothing more than the source of federal policy that courts look to when applying the common law state secrets privilege. But constitutionally-inspired deference to the executive branch is not the same as constitutional law.

In any event, the parties' disagreement over the origins of the state secrets privilege is of little practical significance. Whether a "clear statement," a comprehensive legislative scheme or something less embracing is required, Congress has provided what is necessary for this court to determine that FISA preempts or displaces the state secrets privilege, but only in cases within the reach of its provisions. This is such a case.

C

In addition to their more substantial arguments, defendants advance two arguments why the court should not even take up the issue remanded by the court of appeals. Defendants' first such argument in this regard may be easily dispatched. Defendants argue that the court may not reach the question remanded for consideration by the court of appeals because the court lacks jurisdiction over plaintiffs' claims. Wholly apart from the disregard for the court of appeals——whose decisions bind this court, after all——that acceptance of defendants' argument would entail, defendants' argument lacks merit.

Defendants premise their argument on plaintiffs' lack of standing to obtain prospective relief; that is, because plaintiffs cannot show that they have been injured or face a "real and

immediate threat" of harm in the future, defendants conclude that Article III standing is absent. Doc # 432/17 at 7-8. Plaintiff cannot show injury, contend defendants, because the state secrets privilege prevents the government from confirming or denying that plaintiffs have been subjected to unlawful surveillance.

The circularity of defendants' argument to one side, defendants conflate the state secrets privilege with the "aggrieved person" requirement of section 1810, discussed in Part III infra. If plaintiffs can show that they are "aggrieved" as section 1810 contemplates, then plaintiffs have adequately demonstrated injury for purposes of establishing Article III standing.

Somewhat more substantially, defendants argue that plaintiffs cannot pursue their claims because section 1810 does not waive the United States' sovereign immunity against suits naming the government or individuals acting in their official capacity. Employing a variety of arguments, defendants assert that civil liability under section 1810 is "linked to intentional misconduct by individual federal employees and officials." Doc # 446/29 at 7. They also assert that "[t]he Complaint does not name any of the individual defendants in their individual capacity." Doc # 432 at 9. And they point out that plaintiffs have not served defendants in their individual capacities, an assertion that plaintiffs do not dispute. Doc # 450/31 at 2.

Plaintiffs counter that defendants made similar arguments before the court of appeals but that the court of appeals did not address those points in its disposition of defendants' appeal. Doc # 435/20 at 24. Plaintiffs also contend that for the court to take up this issue and, especially, to entertain defendants' assertion

that governmental immunity bars adjudication of the other issues before the court, would violate the court of appeals' instructions to this court in its order remanding the case. Id.

It is, of course, true that section 1810 does not contain a waiver of sovereign immunity analogous to that in 18 USC section 2712(a) which expressly provides that aggrieved persons may sue the United States for unlawful surveillance in violation of Title III. But FISA directs its prohibitions to "Federal officers and employees" (see, e g, 50 USC §§ 1806, 1825, 1845) and it is only such officers and employees acting in their official capacities that would engage in surveillance of the type contemplated by FISA. The remedial provision of FISA in section 1810 would afford scant, if any, relief if it did not lie against such "Federal officers and employees" carrying out their official functions. Implicit in the remedy that section 1810 provides is a waiver of sovereign immunity.

Of no small moment to this court's consideration of defendants' sovereign immunity contention, it appears that defendants asserted the same argument in the court of appeals which seems simply to have ignored it, presumably as insubstantial or premature given the present state of the record.

In Part IV of this order, the court discusses whether plaintiffs should be granted leave to serve defendants in their individual capacities.

III

The determination that FISA preempts the state secrets privilege does not necessarily clear the way for plaintiffs to

pursue their claim for relief against these defendants under FISA's section 1810. That section provides:

> An aggrieved person, other than a foreign power or an agent of the foreign power * * * who has been subjected to an electronic surveillance or about whom information obtained by electronic surveillance of such person has been disclosed or used in violation of section 1809 of this title shall be entitled to recover——
>
> (a) actual damages * * *
>
> (b) punitive damages; and
>
> (c) reasonable attorney's fees and other investigation and litigation costs reasonably incurred.

50 USC § 1810. An "aggrieved person" is "a person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance." 50 USC § 1801(i). Section 1809, violation of which forms the basis for liability under section 1810, criminalizes two types of conduct: (1) intentionally "engag[ing] in electronic surveillance under color of law except as authorized by statute" and (2)

> disclos[ing] or us[ing] information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance not authorized by statute.

A host of obstacles, however, make section 1810 a mostly theoretical, but rarely, if ever, a practical vehicle for seeking a civil remedy for unlawful surveillance.

A

Before an aggrieved person can bring an action for damages under section 1810, the person must learn somehow of the

electronic surveillance and thus the cause to be "aggrieved." The primary circumstance FISA describes in which a person learns of this surveillance arises from a criminal proceeding——i e, if and when the individual is arrested and charged with a crime. For example, section 1806(c) provides:

> Whenever the Government intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, against an aggrieved person, any information obtained or derived from an electronic surveillance of that aggrieved person pursuant to the authority of this subchapter, the Government shall, prior to the trial, hearing, or other proceeding or at a reasonable time prior to an effort to so disclose or so use that information or submit it in evidence, notify the aggrieved person and the court or other authority in which the information is to be disclosed or used that the Government intends to so disclose or so use such information.

Nearly identical requirements applicable to state governments require notification to the attorney general of the United States as well as to the aggrieved party and the court. § 1806(d). An analogous pair of notification provisions pertaining to evidence obtained pursuant to physical searches applies to the United States and to state governments, respectively. § 1825(d) and (e). See also § 1845(c) and (d)(pertaining to pen registers and trap and trace devices) and 50 USC § 1861(h)(part of the USA PATRIOT Act enacted in 2001 and amended in 2006, pertaining to "information acquired from tangible things").

FISA's section 1806(j) provides for notice to be given to the United States person targeted for surveillance when "an emergency employment of electronic surveillance is authorized under section 1805(e) * * * and a subsequent order approving the surveillance is not obtained." In that circumstance, the judge

"shall cause to be served" on the affected United States persons notice of the fact of the application, the period of the surveillance and "the fact that during the period information was or was not obtained." The notice provided for under section 1806(j) may be postponed or suspended once for up to ninety days upon an ex parte showing of good cause by the government. Upon a further ex parte showing of good cause, the notice requirement under section 1806(j) may be forever waived.

FISA contains a provision requiring direct notification to a "United States person" whose residence has been searched under FISA's section 1824 if "at any time after the search the Attorney General determines there is no national security interest in continuing to maintain the secrecy of the search." 50 USC § 1825(b). In that event, the attorney general "shall provide notice to the United States person * * * of the fact of the search conducted * * * and shall identify any property of such person seized, altered, or reproduced during such search." Id.

**Intelligence-gathering related to national security is generally not for law enforcement; in fact, the initiation of law enforcement actions may work at cross-purposes to the goals of the intelligence-gathering by disrupting surveillance that is more valuable to national security goals if left intact. The sense that intelligence-gathering under FISA was rarely for the purpose of criminal prosecution emerges from the text of FISA as crafted in Congress and from its legislative history. In the context of allowing the destruction of surveillance records acquired under FISA, the Senate Report distinguished FISA from Title III, noting: **

> **Although there may be cases in which information acquired from a foreign intelligence surveillance will be used as evidence of a crime, these cases are expected to be relatively few in number, unlike Title III interceptions the very purpose of which is to obtain evidence of criminal activity. The Committee believes that in light of the relatively few cases in which information acquired under this chapter may be used as evidence, the better practice is to allow the destruction of information that is not foreign intelligence information or evidence of criminal activity. This course will more effectively safeguard the privacy of individuals * * *.**

Foreign Intelligence Surveillance Act of 1978, S Rep No 95-604 Part I, 95th Cong 2d Sess 39 (1978), reprinted in 1978 USCCAN 3940-41. Situations in which individuals subject to FISA warrants would be notified of such warrants are therefore narrowly circumscribed under FISA and this appears to be by design.

FISA also contains reporting requirements to facilitate Congressional oversight of FISA, but these are of little help to an individual seeking to learn of having been the subject of a FISA warrant: sections 1808 (electronic surveillance), 1826 (physical searches), 1846 (pen registers and trap and trace devices) and 1862 (requests for production of tangible things). Each of these provisions, under the heading "Congressional oversight," requires semiannual reporting by the United States attorney general to Congress.

As relevant to the subject matter of the instant action, section 1808(a)(1) requires that the attorney general on a semiannual basis "fully inform" certain Congressional committees "concerning all electronic surveillance under this subchapter." Section 1801(a)(2) requires that each report under section 1808(a)(1) include a description of:

> **(A) the total number of applications made for orders and extensions of orders approving electronic surveillance under this subchapter where the nature and location of each facility or place at which the electronic surveillance will be directed is unknown;**
>
> **(B) each criminal case in which information acquired under this chapter has been authorized for use at trial during the period covered by such report; and**
>
> **(C) the total number of emergency employments of electronic surveillance under section 1805(f) of this title and the total number of subsequent orders approving or denying such electronic surveillance.**

Of note, these provisions only require itemized information about surveillances to be reported to Congress if the information pertains to criminal cases in which the information is intended to be used at trial. All other surveillances and/or uses need be reported in the form of aggregate numbers only.

A further reporting requirement newly adopted in 2004 as part of the Intelligence Reform and Terrorism Prevention Act of 2004, PL 108-458, requires the attorney general to report semiannually to the Congressional intelligence committees:

> **(1) the aggregate number of persons targeted for orders issued under this chamber [broken down by type of warrant or search];**
>
> **(2) the number of individuals covered by an order issued pursuant to [§ 1801(b)(1)(C) (i e non-United States persons who are "agent[s] of a foreign power" engaged in "international terrorism or activities in preparation therefor")];**
>
> **(3) the number of times that the Attorney General has authorized that information obtained under this chapter may be used in a criminal proceeding * * *;**
>
> **(4) a summary of significant legal interpretations of this chapter involving matters before the FISC or the FISCR * * *; and**
>
> **(5) copies of all decisions (not including orders) or opinions of the FISC or FISCR that include**

> significant construction or interpretation of the provisions of this chapter.

50 USC § 1871(a). These reports are presumably not available to the press or the public; in any event, they do not provide any means for an individual to learn of having been subject to surveillance or search under a FISA warrant.

A provision requiring periodic reporting to Congress by the Department of Justice of the number of pen register orders and orders for trap and trace devices applied for under 18 USC § 3123 and under FISA by law enforcement agencies of the Department of Justice was enacted in 1986 as part of the Electronic Communications Privacy Act of 1986, Pub L 99-508, 100 Stat 1871. 18 USC §§ 3121(a), 3126. The report to Congress must include certain specifics as to each order: the period of interceptions, including extensions, the offense, the number of investigations, the number and nature of facilities affected and the identity of the applying agency and the person authorizing the order. Id § 3126. There are, however, no specific notification requirements in that chapter (Chapter 206).

By contrast, Title III, 18 USC §§ 2510-22, the federal wiretapping statute used by law enforcement to conduct electronic surveillance domestically, provides not only for reporting to Congress to facilitate oversight of the executive branch's surveillance activities, but also for notice as a matter of course to individuals surveilled and for civil liability to such individuals in the event of unlawful surveillance.

Reporting to Congress on electronic surveillance under Title III is the responsibility of the judiciary, the Department of

Justice and the individual states' attorneys general. All three are separately and independently obligated to provide data about applications for electronic surveillance to the Administrative Office of the United States Courts, which in turn must transmit annually to Congress "a full and complete report concerning the number of applications for orders and extensions granted or denied pursuant to this chapter during the preceding calendar year." 18 USC § 2519. "The reports are not intended to include confidential material [but] should be statistical in character * * * It will assure the community that the system of court-order electronic surveillance envisioned by the proposed chapter is properly administered * * *." Omnibus Crime Control and Safe Streets Act of 1968, S Rep No 1097, 90th Cong 2d Sess (1968), reprinted in 1968 USCCAN at 2196.

Regarding notice to surveilled individuals, 18 USC section 2518(d) provides that, "within a reasonable time but not later than ninety days after the filing of an application [for interception of electronic communications]," whether successful or unsuccessful, the judge in the matter "shall cause to be served" on the individuals affected "an inventory" notifying them of the fact, date and disposition of the order or application and whether or not wire, oral or electronic communications were intercepted. The statute further authorizes the judge, upon motion by an individual so notified, to allow inspection of "such portions of the intercepted communications, applications and orders as the judge determines to be in the interest of justice." Id. The serving of the inventory may be postponed "on an ex parte showing of good cause * * *." Id.

The legislative history of this provision both acknowledges and addresses the potential implications for national security of section 2518(d)'s notice requirement and expressly contemplates civil actions based on the inventories:

> **[W]here the interception relates, for example, to a matter involving or touching on the national security interest, it might be expected that the period of postponement could be extended almost indefinitely. Yet the intent of the provision is that the principle of postuse notice will be retained. This provision alone should insure the community that the techniques are reasonably employed. Through its operation all authorized interceptions must eventually become known at least to the subject. He can then seek appropriate civil redress for example, under section 2520 * * * if he feels that his privacy has been unlawfully invaded.**

1968 USCCAN at 2194. In describing the civil damages available under section 2520, the Senate report stated that Congress expressly contemplated the provisions requiring notice to affected individuals to form the basis for civil suits: "It is expected that civil suits, if any, will instead grow out of the filing of * * * inventories under section 2518(8)(d)." Id at 2196.

Eighteen USC section 2520, in turn, provides for civil remedies in the form of injunctive relief, declaratory relief and damages and sets out specific measures of damages based on the number of violations ($50-500 for the first finding of liability, $100-1000 for the second and, for the third or other subsequent finding of liability, actual damages and profits reaped or $100 per day or $10,000). 18 USC § 2520(c). Defenses include, inter alia, good faith reliance on a court warrant or order, grand jury subpoena or legislative or statutory authorization. Id.

In summary, FISA makes little provision for notice to surveilled individuals except when the government chooses to

disclose surveillance materials and the provisions that exist are easy for the government to avoid. This must be presumed to be part of Congress's design for FISA because the notification procedure in Title III——which, moreover, contemplated special handling of cases involving national security concerns——predated FISA by a decade. Congress could have modeled FISA on Title III in this regard, but did not do so. In consequence, the cases are few and far between in which an individual ever learns of having been subject to electronic surveillance within FISA's purview and therefore possibly having standing as an aggrieved party for FISA section 1810 purposes.

One of the few cases in which an individual surveilled under a FISA warrant became aware of his status as an "aggrieved party" is that of Brendan Mayfield, an American-born United States citizen, attorney and former United States Army officer who brought suit against the United States after being arrested and imprisoned in 2004 upon suspicion of involvement in the conspiracy to detonate bombs on commuter trains in Madrid, Spain. Mayfield v United States, 504 F Supp 2d 1023 (D Or 2007). The Mayfield case is instructive. The investigation leading to the arrest and the arrest itself were apparently the result of a false fingerprint match which led the FBI, among other things, to seek and obtain from the FISC an order authorizing electronic surveillance of Mayfield's home and his law office. Id at 1028. The published opinion in Mayfield noted, without providing specifics, that Mayfield had settled claims for "past injuries," id at 1033; Mayfield, however, continued to press his claims for a declaration that FISA, as amended by the USA PATRIOT Act, violated the Fourth

Amendment by undermining the requirement of probable cause as a pre-condition for obtaining a search warrant and for collecting, disseminating and retaining information thus obtained. Mayfield also claimed that FISA violated the Fourth Amendment by permitting warrants to be issued under FISA without a showing that the "primary purpose" of the search is to obtain foreign intelligence information. Id at 1032.

The district court agreed with Mayfield and granted, on summary judgment, a declaration finding FISA unconstitutional. The United States appealed this order and the appeal is now pending before the court of appeals.

The district court drew particular attention to the "notice problem" under FISA:

> Nor does FISA require notice. The Fourth Amendment ordinarily requires that the subject of a search be notified that the search has occurred. Although in some circumstances the government is permitted to delay the provision of notice, the Supreme Court has never upheld a statute that, like FISA, authorizes the government to search a person's home or intercept his communications without ever informing the person that his or her privacy has been violated. Except for the investigations that result in criminal prosecutions, FISA targets never learn that their homes or offices have been searched or that their communications have been intercepted. Therefore, most FISA targets have no way of challenging the legality of the surveillance or obtaining any remedy for violations of their constitutional rights.

Id at 1039.

Ironically, the Mayfield case seems an ideal one for the government to provide notification under section 1825(b), discussed above, which directs the attorney general to notify United States persons whose residences have been subjected to physical search after the attorney general "determines there is no national

security interest in continuing to maintain the secrecy of the search." Yet the government leaned toward secrecy rather than candor. Only after Mayfield had filed litigation and moved to compel notification did the government notify him of the physical search and, in doing so, contended that both the fact and the extent of notification were entirely within the attorney general's discretion. Agency Defendants' Reply In Support Of Motion to Dismiss Counts Twelve and Thirteen and Opposition to Motion to Compel, Mayfield v Gonzales, CV 04-1427-AA Doc # 72 at 6-10, United States District Court for the District of Oregon, filed April 15, 2005. Mayfield later challenged the sufficiency of the government's disclosure. Mayfield v Gonzales, 2005 WL 1801679, *17 (D Or 2005). The Mayfield case illustrates the limited effectiveness of FISA's narrowly-defined notice provision relating to physical searches. Limited and imperfect as FISA's notification provision for physical searches may be, FISA contains no comparable provision for United States persons who have been subjected to electronic surveillance as opposed to physical search.

In the Al-Haramain case, notification to plaintiffs of their potential status as "aggrieved parties" came in the form of an accident: the inadvertent disclosure of the Sealed Document during discovery proceedings, a disclosure that the various United States entities involved took immediate and largely successful steps to undo. To speak metaphorically, the inadvertent disclosure by OFAC of the Sealed Document amounted to a small tear in the thick veil of secrecy behind which the government had been conducting its electronic surveillance activities. The Oregon district court refused to allow plaintiffs to learn more by

conducting discovery, but held that no further harm could result from working with the salient information divulged thus far. By refusing to allow the use of the Sealed Document in any form for the adjudication of plaintiffs' claims in this matter, the court of appeals required that the small tear be stitched closed, leaving plaintiffs with actual but not useful notice and without the sole item of evidence they had offered in support of their claims.

B

Difficult as it is to learn of one's status as an aggrieved party for section 1810 purposes, an aggrieved party needs more than mere knowledge of the surveillance to be able to proceed with a lawsuit under section 1810. The next major obstacle to seeking civil remedies under FISA is the lack of a practical vehicle for obtaining and/or using admissible evidence in support of such claims. An aggrieved party must be able to produce evidence sufficient to establish standing to proceed as an "aggrieved party" and, later, to withstand motions for dismissal and/or summary judgment. This effort is encumbered with legal and practical obstacles.

As noted above in Part III A, FISA does not provide for the preservation of recordings and other information obtained pursuant to a FISA warrant. Rather, Congress intended to allow such material to be destroyed, the idea being that to allow destruction would better protect the privacy of individuals surveilled than to require preservation. S Rep No 95-604 Part I at 39. By contrast, Title III expressly requires intercepted communications to be recorded and expressly prohibits destruction

of the recordings except upon an order of the issuing or denying judge. Also, "in any event [they] shall be kept for ten years." 18 USC § 2518(8)(a). It provides, moreover, that "custody of the recordings shall be wherever the judge orders." Id. These provisions ensure that a body of evidence establishing the fact of the surveillance is brought into existence and safeguarded under a a judge's control. By failing to impose parallel obligations on the government agencies and officials who are the putative defendants in an action alleging FISA violations, FISA provides little help to "aggrieved persons" who might seek to become civil plaintiffs.

Plaintiffs and plaintiff amici contend that FISA's section 1806(f) provides the means for them to overcome this evidentiary hurdle. The court has carefully studied section 1806(f) and does not agree.

As relevant here, section 1806(f) provides:

> whenever any motion or request is made by an aggrieved person pursuant to any other statute or rule of the United States * * * before any court * * * of the United States * * * to discover or obtain applications or orders or other materials relating to electronic surveillance or to discover, obtain, or suppress evidence or information obtained or derived from electronic surveillance under this chapter, the United States district court * * * shall, notwithstanding any other law, if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States, review in camera and ex parte the application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted. In making this determination, the court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance.

The parties have argued at length in their papers and in court about the meaning and application of this convoluted pair of sentences. Both plaintiff amici and telecommunications carrier defendant amici ("defendant amici") have devoted their entire amicus briefs to this subject. Doc # 440/23, 442/25.

Defendants contend that section 1806(f) does not come into play unless and until the government has acknowledged that it surveilled the "aggrieved person" in question (by, for example, initiating criminal proceedings), but that it is not available as a means for an individual to discover having been surveilled absent such governmental acknowledgment. See, e g, Doc #432/17 at 16-20. Defendants further assert that, assuming arguendo that FISA "preempts" the state secrets privilege, as this court holds it does for purposes of electronic surveillance, plaintiffs would still be unable to establish their standing as "aggrieved persons" for section 1810 purposes without "inherently risk[ing] or requir[ing] the disclosure of state secrets to the plaintiffs and the public at large." Id at 22-23.

The defendant amici present more detailed arguments about section 1806(f) that are in accord with defendants' position. They assert that the "motion * * * to discover" provision at issue in this case "creates no rights for aggrieved persons; it provides procedures to implement their existing right to seek discovery in support of efforts to suppress evidence obtained or derived from electronic surveillance." Doc #442/25 at 5. Defendant amici further assert that section 1806(f)'s purpose was to preserve for the prosecution a "dismiss option" when the legality of surveillance evidence is challenged, so that the prosecution could

choose not to proceed rather than risk the disclosure of classified information. Id at 10-11. In support of this contention, they point to section 1806(f)'s language providing for the United States attorney general to invoke its procedures and argue that the section does not provide for courts to compel the disclosure of information absent the attorney general's involvement. Id at 11.

Defendant amici also contrast FISA's section 1806(f) with 18 USC section 3504(a)(1), enacted in 1970 as part of the Organized Crime Control Act. The latter establishes a procedure by which "a party aggrieved" seeking to exclude evidence based on a claim that it was obtained illegally may obligate "the opponent of the claim" (i e, the government) "to affirm or deny the occurrence of the alleged unlawful act." Defendant amici argue that "[t]he existence of the carefully circumscribed discovery right in § 3504 negates any suggestion that § 1806(f) implicitly covers the same ground" and cite United States v Hamide, 914 F2d 1147 (9th Cir 1990) for the proposition that section 3504(a) and section 1806(f) can be used together but that they accomplish different objectives and cannot be construed as serving similar purposes. Doc # 442/25 at 15-16.

In Hamide, an immigration judge had entertained a motion under section 3504(a)(1) by an individual in deportation proceedings requesting that the government affirm or deny the existence of electronic surveillance. After the government disclosed that it had conducted electronic surveillance of the individual, it filed in the district court a "Petition of the United States for Judicial Determination of Legality of Certain Electronic Surveillance" under FISA's section 1806(f), together with the FISA materials relevant to the authorization of the surveillance filed under seal and a request

that the matter be handled ex parte for national security reasons. 914 F2d at 1149. The district court then ruled ex parte in the government's favor. Id at 1149-50.

Defendant amici argue that Congress could have incorporated into FISA a procedure like that provided for in section 3504(a)(1) by which an individual could require the executive branch to confirm or deny the existence of electronic surveillance and, since Congress did not do so, it must be presumed not to have intended such a procedure to be available under FISA. Doc #442/25 at 16.

Plaintiff amici counter defendants' arguments against plaintiffs' proposed use of section 1806(f) with several major contentions. First, they argue that section 1806(f)'s scope is expansive enough to provide for in camera review in any civil or criminal case——not merely cases arising under FISA——in which a claim of unlawful surveillance is raised. Doc #440/23 at 11-13, 17. They point out that the text of section 1806(f) referring to "any motion or request * * * pursuant to any other statute or rule of the United States" does not suggest a limitation to criminal statutes. Id at 11. They also point to language in the conference report on the final version of FISA stating "[t]he conferees agree that an in camera and ex parte proceeding is appropriate for determining the lawfulness of electronic surveillance in both criminal and civil cases." Id at 13, citing H Conf Rep 95-1720 at 32. And plaintiff amici find support in the District of Columbia Circuit's opinion in ACLU Foundation of Southern California v Barr, 952 F2d 457, 465 n 7 (D C Cir 1991), which cited FISA's legislative history for the proposition that Congress had intended a court's in

camera, ex parte review under section 1806(f) to "determine whether the surveillance was authorized and conducted in a manner that did not violate any constitutional or statutory right." Thus, plaintiff amici contend, section 1810 is one such "other statute" referred to in section 1806(f) under which in camera review is available.

Next, plaintiff amici characterize defendants' contention that section 1806(f) is only available in cases in which the government has acknowledged having surveilled a party as "look[ing] at section 1806(f) through the wrong end of the telescope." Doc #440/23 at 14. Plaintiff amici correctly observe that section 1806(f) only comes into play when the attorney general notifies the court that "disclosure or an adversary hearing would harm the national security"——for example, in opposing a discovery request. A "motion or request * * * by an aggrieved person" alone is not sufficient to trigger in camera review. Therefore, they argue, defendants' position that the government must have acknowledged surveillance sets the bar higher than FISA prescribes.

Third, plaintiff amici address what they believe the bar should be——that is, what an individual must show to establish being "aggrieved" for section 1806(f) purposes. They assert that a person need only have a "colorable basis for believing he or she had been surveilled." Doc #440/23 at 11-16. Lacking examples arising directly under section 1806(f), plaintiff amici look to cases decided under 18 USC section 3504(a)(1) (discussed above), including United States v Vielguth, 502 F2d 1257, 1258 (9th Cir 1974). In Vielguth, the Ninth Circuit held that the government's obligation to affirm or deny the occurrence of electronic

surveillance under section 3504(a)(1) "is triggered by the mere assertion that unlawful wiretapping has been used against a party." Plaintiff amici argue that the standard articulated in Vielguth is the applicable standard for an "aggrieved person" for purposes of FISA's section 1806(f). Doc #440/23 at 16.

The court agrees with plaintiffs that section 1806(f) is not limited to criminal proceedings, but may also be invoked in civil actions, including actions brought under section 1810. The court disagrees with defendants' proposed limitation of section 1806(f) to cases in which the government has acknowledged the surveillance at issue. The plain language of the statute, which the court must use as its primary compass, United States v Ron Pair Enterprises, Inc, 489 US 235, 242 (1988), does not support defendants' purported limitations.

The court parts company with plaintiffs, however, with regard to what an individual must show to establish being "aggrieved" for section 1806(f) purposes and, consequently, the availability of section 1806(f) to plaintiffs in this case in its current posture. As the court reads section 1806(f), a litigant must first establish himself as an "aggrieved person" before seeking to make a "motion or request * * * to discover or obtain applications or orders or other materials relating to electronic surveillance [etc]." If reports are to be believed, plaintiffs herein would have had little difficulty establishing their "aggrieved person" status if they were able to support their request with the Sealed Document. But the court of appeals, applying the state secrets privilege, has unequivocally ruled that plaintiffs in the current posture of the case may not use "the

Sealed Document, its contents, and any individuals' memories of its contents, even well-reasoned speculation as to its contents." 507 F3d at 1204. Pplaintiffs must first establish "aggrieved person" status without the use of the Sealed Document and may then bring a "motion or request" under § 1806(f) in response to which the attorney general may file an affidavit opposing disclosure. At that point, in camera review of materials responsive to the motion or request, including the Sealed Document, might well be appropriate.

The court disagrees with plaintiff amici's suggestion that Vielguth, an opinion that established a claimant's burden to invoke 18 USC section 3504(a)(1), should also be relied on to define the burden for an individual to establish standing as an "aggrieved person" for purposes of FISA section 1806(f). The bar set by Vielguth is too low given the text and structure of FISA. Moreover, a review of other Ninth Circuit cases reveals that Vielguth did not define the standard for all purposes under section 3504(a)(1). The court in Vielguth was at pains to distinguish its earlier decision in United States v Alter, 482 F2d 1016 (9th Cir 1973), which, while stating that a witness "does not have to plead and prove his entire case to establish standing and to trigger the Government's responsibility to affirm or deny," nonetheless established a stringent test for making out a prima facie issue of electronic surveillance of counsel for a grand jury witness. The court held required affidavits that established:

> (1) the specific facts which reasonably lead the affiant to believe that named counsel for the named witness has been subjected to electronic surveillance;
>
> (2) the dates of such suspected surveillance;

> (3) the outside dates of representation of the witness by the lawyer during the period of surveillance;
>
> (4) the identity of the person(s), by name or description, together with their respective telephone numbers, with whom the lawyer (or his agents or employees) was communicating at the time the claimed surveillance took place; and
>
> (5) facts showing some connection between possible electronic surveillance and the grand jury witness who asserts the claim or the grand jury proceeding in which the witness is involved.

Id at 1026. Vielguth distinguished Alter by limiting the latter to "a claim by the person under interrogation that questions put to him are tainted by unlawful surveillance of conversations in which he did not participate" and did so only over the dissent of one of the three panel members. 502 F2d at 1259-61.

Not long after Vielguth, the Ninth Circuit clarified the standard, but only slightly. In United States v See, 505 F2d 845, 855-56 (9th Cir 1974), the court rejected a claim under section 3504 as "vague to the point of being a fishing expedition" and held that correspondingly little was required of the government. The court noted that "a general claim requires only a response appropriate to such a claim" and that "varying degrees of specificity in a claim will require varying degrees of specificity in a response." Id at 856 & n 18.

The flexible or case-specific standards articulated by the Ninth Circuit for establishing aggrieved status under section 3504(a)(1), while certainly relevant, do not appear directly transferrable to the standing inquiry for an "aggrieved person" under FISA. While attempting a precise definition of such a standard is beyond the scope of this order, it is certain that

plaintiffs' showing thus far with the Sealed Document excluded falls short of the mark. Plaintiff amici hint at the proper showing when they refer to "independent evidence disclosing that plaintiffs have been surveilled" and a "rich lode of disclosure to support their claims" in various of the MDL cases. Doc #440 at 16-17. To proceed with their FISA claim, plaintiffs must present to the court enough specifics based on non-classified evidence to establish their "aggrieved person" status under FISA.

C

It is a testament to the obstacles to seeking civil remedies for alleged violations of FISA that section 1810 has lain "dormant for nearly thirty years." Andrew Adler, Note, The Notice Problem, Unlawful Electronic Surveillance, and Civil Liability Under the Foreign Intelligence Surveillance Act, 61 U Miami L Rev 393, 397 (2006-07). Dormant indeed. The print version of the United States Code Annotated contains no case notes under section 1810. The parties have cited no other case in which a plaintiff has actually brought suit under section 1810, let alone secured a civil judgment under it. By contrast, the civil liability provisions of Title III, 18 USC § 2520, have been used successfully by "aggrieved persons" with regularity since they were enacted in 1968. See, e g, Jacobsen v Bell Telephone Co, 592 F2d 515 (9th Cir 1978), Dorris v Absher, 179 F3d 420 (6th Cir 1999).

While Congress enacted section 1810 in order to provide a private cause of action for unlawful surveillance, section 1810 bears but faint resemblance to 18 USC section 2520. While the court must not interpret and apply FISA in way that renders section

1810 superfluous, Dole Food Co v Patrickson, 538 US 468, 476-77 (2003), the court must be wary of unwarranted interpretations of FISA that would make section 1810 a more robust remedy than Congress intended it to be. As noted, Title III predated FISA by a full decade. If Congress had so intended, it could have written FISA to offer a more fulsome and accessible remedy patterned on Title III. Congress may therefore be presumed to have intended not to provide such a remedy and the court should not strain to construe FISA in a manner designed to give section 1810 greater effect than Congress intended. See id. The same applies with regard to the procedure set forth in 18 USC section 3504(a)(1), enacted in 1970. This is not to say that it is impossible to obtain relief under section 1810, but the fact that no one has ever done so reinforces the court's reading of the plain terms of the statute: section 1810 is not user-friendly and the impediments to using it may yet prove insurmountable.

IV

On April 17, 2008, less than a week before the hearing on defendants' second motion to dismiss, plaintiffs filed a motion for an order extending the time to serve defendants Bush, Alexander, Werner and Mueller individually, presumably in response to defendants' sovereign immunity arguments in their moving and reply papers. Doc # 447/30. In that motion, plaintiffs do not specifically state whether they intended to sue defendants in both their official and individual capacities, but they assert that "a nonspecific complaint may be characterized as alleging both official and personal capacity liability." Id at 2. Plaintiffs

explain their failure to serve the individual defendants individually within the 120-day deadline for service under Federal Rule of Civil Procedure 4(m) as follows: "Within weeks [of serving their complaint upon the Attorney General] this case became focused on the classified document that Plaintiffs filed under seal with the Complaint." Id at 1. They assert that issues pertaining to the Sealed Document, including defendants' assertion of the state secrets privilege, "have driven this litigation to date in the trial and appellate courts and have overshadowed all other aspects of this case." Id.

Plaintiffs also contend that the individual defendants will not be prejudiced by late service of the complaint because: (1) they have been on notice of the litigation either through personal, open participation in the defense (e g, Declaration of NSA Director & Declaration of Keith B Alexander, Al-Haramain, No C 06-0274 KI Doc #55-2, 59, United States District Court for the District of Oregon, filed June 21, 2006) or due to the large amount of publicity surrounding these cases and (2) because the case has advanced little due to the courts' focus on the Sealed Document, the state secrets privilege and legal issues under FISA. Doc #447/30 at 2-3.

Defendants vigorously oppose plaintiffs' motion, asserting that plaintiffs have failed to establish "good cause" warranting relief from the 120-day deadline. They assert that plaintiffs have been on notice of the defendants' sovereign immunity defense for well over a year and of the particular point that individual defendants had not been served for "at least nine months." Doc # 448/31 at 3. Defendants assert that they will be

prejudiced by the proposed late service because the suit has been pending and actively litigated without notice to defendants as individuals for over two years. Id at 5.

Defendants also point out——correctly——that plaintiffs' motion is not in accordance with this court's local rules as it was filed less than one week before the April 23 hearing without a hearing date specified on the moving papers. Defendants filed a short opposition the day before the hearing requesting, inter alia, that the motion be placed on the calendar and briefed in accordance with the local rules.

Plaintiffs' motion mentions Civil Local Rule 6-3 (Doc # 447/30 at 1), but does not properly invoke or comply with it. Rule 6-3 provides the procedure for obtaining a hearing on shortened time. It requires the filing of a motion to shorten time and sets forth detailed requirements for such a motion. Plaintiffs filed no such motion. On the other hand, plaintiffs did not expressly seek to have their motion heard on shortened time and, at the April 23 hearing, it was defendants' attorney who first sought to be heard on the matter. Hearing transcript, Doc # 452 at 44-45.

Notwithstanding the inartful manner in which plaintiffs brought their motion, the court finds the briefing and arguments for and in opposition to plaintiffs' motion adequate. No further briefing on this matter will be required. Plaintiffs, however, are admonished to review the local rules of this court and to abide by them for the duration of this litigation.

Rule 4(m) provides two alternative courses for a court to follow if a plaintiff has failed to serve one or more defendants within the 120-day time limit. As something like 680 days had

elapsed between plaintiffs' filing of their action and the date of their motion for an extension of time to serve the individual defendants individually, plaintiffs have indisputably exceeded the 120-day limit by a wide margin. Rule 4(m) requires the court to dismiss the action without prejudice against the particular defendants in question "or order that service be made within a specified time." If plaintiff shows good cause for the failure, however, the court "must extend the time for service for an appropriate period." The determinations required to adjudicate the motion for an extension of time to serve defendants are committed to the discretion of the court. Puett v Blandford, 912 F2d 270, 273 (9th Cir 1990).

The court agrees with plaintiffs that although more than two years have elapsed, little has occurred in the litigation that would prejudice a late-served individual defendant. This is particularly the case given the specific individuals at issue, all of whom are high-level government officials closely and publicly connected to the policies and practices at issue in this litigation. Dismissal on the ground of failure to serve individual defendants would needlessly complicate the litigation and would not advance the interests of justice in this case. Without reaching the question whether plaintiffs have established "good cause" for their failure to serve the individual defendants, the court instead GRANTS the motion to extend time for service. Should plaintiffs choose to amend their complaint in accordance with this order, they may serve all unserved defendants with their amended complaint within fifteen (15) days of filing it with the court.

****

V

The lack of precedents under section 1810 complicates the task of charting a path forward. The court of appeals reversed the Oregon district court's plan for allowing plaintiffs to proceed with their suit, but did not suggest a way for plaintiffs to proceed without using the Sealed Document. Nonetheless, the court believes that dismissal with prejudice is not appropriate. Accordingly, plaintiffs' FISA claim will be dismissed with leave to amend. Plaintiffs should have the opportunity to amend their claim to establish that they are "aggrieved persons" within the meaning of 50 USC § 1801(k). In the event plaintiffs meet this hurdle, the court will have occasion to consider the treatment of the Sealed Document under section 1806(f) and the significant practical challenges of adjudicating plaintiffs' claim under section 1810.

For the reasons stated herein, plaintiffs' claim under FISA is DISMISSED with leave to amend. Plaintiffs shall have thirty (30) days to amend their complaint in accordance with this order. Should plaintiffs seek to amend their non-FISA claims, they shall do so by means of a noticed motion before this court in accordance with the local rules.

IT IS SO ORDERED.

VAUGHN R WALKER
United States District Chief Judge