Exhibit 8

CASE NO.: 06-17132, 06-17137

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

TASH HEPTING, GREGORY HICKS, CAROLYN JEWEL, AND ERIK KNUTZEN, ON BEHALF OF THEMSELVES AND ALL OTHERS SIMILARLY SITUATED,

PLAINTIFFS-APPELLEES,

V.

AT&T CORP.,

DEFENDANT-APPELLANT, AND

THE UNITED STATES,

INTERVENOR AND APPELLANT.

APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA
THE HONORABLE VAUGHN R. WALKER, CHIEF DISTRICT JUDGE

CIVIL NO. C-06-0672-VRW

BRIEF *AMICUS CURIAE* OF PEOPLE FOR THE AMERICAN WAY FOUNDATION IN SUPPORT OF PLAINTIFFS-APPELLEES

SAMUELSON LAW, TECHNOLOGY & PUBLIC POLICY CLINIC
UNIVERSITY OF CALIFORNIA—BERKELEY SCHOOL OF LAW (BOALT HALL)
JACK I. LERNER (220661)
DEIRDRE K. MULLIGAN (218804)
396 Simon Hall
Berkeley, CA 94720-7200
Telephone: (510) 642-7515
Facsimile: (510) 643-4625

Counsel for *Amicus Curiae*

On the Brief:
JUDITH E. SCHAEFFER
PEOPLE FOR THE AMERICAN WAY FOUNDATION
2000 M Street, NW, Suite 400
Washington, DC 20036
Telephone: (202) 467-4999
Facsimile: (202) 293-2672

TABLE OF CONTENTS

CORPORATE DISCLOSURE STATEMENT

Pursuant to Rule 26.1 of the Federal Rules of Appellate Procedure, *Amicus Curiae* People for the American Way Foundation certifies that no publicly held corporation or other publicly held entity owns 10% or more of People for the American Way Foundation.

DATED: May 2, 2007

By:

_____

SAMUELSON LAW, TECHNOLOGY
& PUBLIC POLICY CLINIC
UNIVERSITY OF CALIFORNIA—BERKELEY
SCHOOL OF LAW (BOALT HALL)
JACK I. LERNER (220661)
DEIRDRE K. MULLIGAN (218804)
396 Simon Hall
Berkeley, CA 94720-7200
Telephone: (510) 642-7515
Facsimile: (510) 643-4625

Counsel for *Amicus Curiae*

TABLE OF AUTHORITIES

CASES

STATUTES

LEGISLATIVE MATERIALS[*]

[*] For a compendium of legislative history materials relating to the Foreign Intelligence Surveillance Act of 1978, please see *Foreign Intelligence Surveillance Act (FISA), available at* http://www.cnss.org/fisa.htm (last visited May 1, 2007).

OTHER AUTHORITIES

INTEREST OF *AMICUS CURIAE*

People For the American Way Foundation ("PFAWF") is a non-partisan, non-profit citizen organization established to promote and protect civil and constitutional rights. Founded in 1980 by a group of civic, religious, and educational leaders devoted to our nation's heritage of tolerance, pluralism, and liberty, PFAWF now has more than 1,000,000 activists and other supporters nationwide, including more than 263,000 in the Ninth Circuit and more than 178,000 in the State of California alone. One of PFAWF's primary missions is to educate the public on the vital importance of our nation's tradition of liberty and freedom, and to defend that tradition through research, advocacy, outreach, and litigation.

This case is of particular concern to PFAWF and its members given the organization's longstanding concern for and defense of civil liberties, and given the breadth of the electronic surveillance that has been alleged. Independent of this litigation, PFAWF has conducted extensive research on the Foreign Intelligence Surveillance Act of 1978 ("FISA") and undertaken a public education initiative addressing legal and policy issues raised by the government's recently disclosed surveillance programs. PFAWF is filing this brief on behalf of its members to highlight for the Court FISA's historical

context and Congress's intent as expressed at the time of the legislation's drafting and passage.

All parties have consented to the filing of this brief. No counsel for a party authored this brief in whole or in part, and no person or entity other than *Amicus Curiae*, or its counsel, made a monetary contribution to the preparation or submission of this brief.[1]

[1] Students of the University of California—Berkeley School of Law (Boalt Hall) Samuelson Law, Technology & Public Policy Clinic (Andy Gass, Yaser Herrera, and Elvin Lee) helped to prepare this brief under the supervision of Jack I. Lerner and Deirdre K. Mulligan.

SUMMARY OF THE ARGUMENT

Appellants aim to subvert Congress's carefully crafted balance between civil liberties and the need for secrecy in litigation over foreign intelligence surveillance initiatives and replace it with a scheme of unrestrained administrative discretion that would allow the President to dictate single-handedly when and how the public can be subject to surveillance in the name of national security. The legislative history of FISA shows that, provoked by revelations of gross civil liberties abuses perpetrated by administrations throughout the post-World War II era, Congress passed FISA to prescribe the "exclusive means" by which the Executive could conduct electronic surveillance for foreign intelligence purposes, as well as the exclusive means by which government concerns for national security in the course of litigation over electronic surveillance should be addressed.

FISA's legislative history reveals that Congress deliberated the precise legal question before the Court in this appeal—whether the need for secrecy around electronic surveillance conducted for national security purposes should bar a civil suit against a telephone company for illegal cooperation with Executive foreign intelligence gathering—and decided that it should not. Congress rejected arguments that the Executive's concerns for secrecy trump the need to protect civil liberties altogether, and crafted a set of exclusive

procedures governing the evaluation of sensitive evidence by district court judges.

Understanding that the Executive could place enormous pressure on private parties to cooperate with foreign intelligence surveillance activities, Congress created a comprehensive framework of procedural protections and remedies to counter-balance this risk. As the legislative history demonstrates, this regime reflected two policy goals: to prevent unlawful surveillance, and to ensure that private parties would be held accountable for assisting with unlawful surveillance. The Congressional committees most directly involved in drafting FISA articulated these policy goals in deliberations that led to two important provisions in FISA: first, exclusive procedures by which judges should weigh evidence that might threaten national security if disclosed in litigation, codified at 50 U.S.C. § 1806(f); and second, provisions establishing the circumstances under which private parties such as phone companies will be liable for unauthorized cooperation with government surveillance efforts, codified at 18 U.S.C. §§ 2511(2)(a)(ii) and 2520.

Congress's decision to allow civil suits against private parties in federal court subject to these additional procedures is particularly important in cases such as this, where the government has admitted that it has circumvented FISA's pre-surveillance approval process. If the Executive is now permitted to

quash this litigation via the state secrets privilege or the *Totten/Tenet* bar, it will have avoided any judicial review whatsoever, in direct contravention of Congress's legislative intent and our constitutional system of checks and balances. As Senator Charles Mathias, Jr., one of FISA's co-sponsors, argued during a 1974 hearing, judicial oversight of electronic surveillance conducted for foreign intelligence gathering purposes is a critical part of any free society:

> If the executive branch believes that the Congress and the courts cannot be trusted to act responsibly on all matters of public policy including those loosely called "national security," then for all practical purposes, the constitutional system of government has been rejected and replaced by an executive national security state.
>
> If it is the view of the Justice Department and the executive branch that the Congress and the courts are not equipped or competent to handle the problems of national security then ways must be devised to make them competent and means provided to equip them to handle such matters; the alternative is authoritarian rule.

Electronic Surveillance for National Security Purposes: Hearings on S. 2820, S.3440, and S.4062 Before the Subcomms. on Criminal Laws and Procedures and Constitutional Rights of the S. Comm. on the Judiciary, 93rd Cong. 255 (1974) [hereinafter *1974 S. Judiciary Comm. Hearings*].

In light of this history, Appellants' assertion of the state secrets privilege and the *Totten/Tenet* bar should be recognized as an attempt to upend the comprehensive, and exclusive, regime that the Senate Judiciary Committee called "a fair and just balance between protection of national security and

protection of personal liberties" shortly before the Senate passed FISA by a vote of ninety-five to one. S. Rep. No. 95-604(I), at 7 (1977).

FACTUAL BACKGROUND

In 1978, Congress enacted FISA in response to revelations of widespread abuses of the Executive's power to conduct electronic surveillance for national security purposes. These abuses were attributed, in part, to Congress's decision to exempt foreign intelligence and national security surveillance from domestic electronic surveillance legislation enacted in 1968.[2] *See generally*, Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, § 802, 82 Stat. 197, 212-223 (codified as amended at 18 U.S.C. §§ 2510-2520 (2006)) ("Title III"); *see also* 18 U.S.C. § 2511(3) (1968) (repealed by FISA, Pub. L. No. 95-511, § 201(c), 97 Stat. 1783, 1797); S. Rep. No. 95-604(I), at 7.

The misconduct that led to FISA's passage came to light in the mid-1970s when a Congressional task force known as the Church Committee produced a series of investigative reports that documented a staggering amount of unlawful surveillance carried out in the name of national security. As the Senate Judiciary Committee concluded, in the years prior to FISA,

[2] In 1972, the Supreme Court held that Title III did not address national security surveillance but indicated that where prior judicial approval is required for surveillance, such approval could be regulated by "such reasonable standards as Congress may prescribe." *United States v. U.S. Dist. Court (Keith)*, 407 U.S. 297, 302-08, 324 (1972).

"surveillance was often conducted by illegal or improper means" and focused on a grossly over-inclusive set of targets, including "a United States Congressman, Congressional staff member, journalists and newsmen, and numerous individuals and groups who engaged in no criminal activity and who posed no genuine threat to the national security." S. Rep. No. 95-604(I), at 8 (quoting S. Select Comm. to Study Governmental Operations with Respect to Intelligence Activities, *Intelligence Activities and the Rights of Americans (Book II)*, S. Rep. No. 94-755, at 12 (1976)). Senator Kennedy explained at the time that "[e]ach [of these initiatives] was undertaken under the catch-all phrase of 'national security.'" *Warrantless Wiretapping and Electronic Surveillance - 1974: J. Hearings Before the Subcomm. on Administrative Practice and Procedure and the Subcomm. on Constitutional Rights of the S. Comm. on the Judiciary and the Subcomm. on Surveillance of the S. Comm. on Foreign Relations*, 93rd Cong. 2 (1974).

The Church Committee devoted substantial attention to a program that bears a striking resemblance to the activities alleged in this case—a long-running effort to create a dragnet targeting international telegrams sent by United States citizens:

> SHAMROCK is the codename for a special program in which [the National Security Agency ("NSA")] received copies of most international telegrams leaving the United States between August

> 1945 and May 1975. Two of the participating international telegraph companies—RCA Global and ITT World Communications—provided virtually all their international message traffic to NSA. The third, Western Union International, only provided copies of certain foreign traffic from 1945 until 1972. SHAMROCK was probably the largest governmental interception program affecting Americans ever undertaken. Although the total number of telegrams read during its course is not available, NSA estimates that in the last two or three years of SHAMROCK's existence, about 150,000 telegrams per month were reviewed by NSA analysts.

S. Select Comm. to Study Governmental Operations with Respect to Intelligence Activities, *Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans (Book III)*, S. Rep. No. 94-755, at 765.[3] The committee determined that operation SHAMROCK likely violated the Fourth Amendment, the Communications Act of 1934, and the controlling National Security Council Intelligence Directive. *Id.* at 765-66; *see generally id.* at 765-776 (describing SHAMROCK in more detail). More generally, the Committee ultimately concluded that "[t]he Constitutional system of checks and balances," without additional statutory protections, "has not adequately controlled intelligence activities." *Intelligence Activities and the Rights of Americans (Book II)*, S. Rep. No. 94-755, at 6.

[3] As technology improved, the NSA developed the ability to sort electronically the telegrams it received under SHAMROCK. *Id.* at 766. The agency could filter out the communications of Americans on certain "watch lists" and circulate them to other intelligence agencies. *Id.* The NSA disguised its involvement in the maintenance of such "watch lists" via another top-secret program discussed in the Church Committee report, Operation MINARET. *Id.* at 749.

FISA embodies Congress's reaction to the Executive's abuse of the "national security" rationale as a means to conduct questionable or outright illegal surveillance. The Senate Judiciary Committee called the legislation "a response to… revelations that warrantless electronic surveillance in the name of national security has been seriously abused," and explained that it crafted this comprehensive set of substantive and procedural constraints in order to "provide the secure framework by which the Executive branch may conduct legitimate electronic surveillance for foreign intelligence purposes." S. Rep. No. 95-604(I), at 15.

Indeed, Congress was very clear about its intent to prohibit the Executive from conducting electronic surveillance of this type other than within FISA's framework. The House and Senate Conference Committee rejected narrow language that would have provided that FISA was merely the "exclusive *statutory* means by which electronic surveillance" for foreign intelligence purposes could be conducted (emphasis added), and instead adopted the Senate bill's broader requirement that FISA would establish the "exclusive means" for such surveillance. H.R. Rep. No. 95-1720, at 35 (1978) (Conf. Rep.) (citing *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 637 (1952) ("[w]hen a President takes measures incompatible with the express or implied will of Congress, his power is at the lowest ebb")). FISA represents "a recognition by

both the Executive branch and the Congress that the statutory rule of law must prevail in the area of foreign intelligence surveillance." S. Rep. No. 95-604(I), at 7.

Congress crafted the details of FISA's regulatory framework over several years, beginning with hearings in April 1974 and concluding with a Conference bill in October 1978—an extensive legislative process that generated thousands of pages of transcripts, reports, case law analysis, and other historical materials. Since enacting FISA in 1978, Congress has several times amended the sections of the U.S. Code where FISA was codified[4]—most notably via the Electronic Communications Privacy Act in 1986 and the USA PATRIOT Act in 2001. *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (amending 18 U.S.C. §§ 2510-22); USA PATRIOT Act of 2001, Pub. L. No. 107-56, § 206-08, 115 Stat. 272, 282-283 (amending 50 U.S.C. §§ 1803-5, 1823). Even with these changes, the procedural framework that Congress created with FISA—provisions for judicial approval of prospective surveillance, subsequent judicial review of its legality, and criminal and civil liability[5]—survives essentially intact to this day. *See* Peter Swire, The System

[4] FISA was codified at 50 U.S.C §§ 1801-11, 18 U.S.C. §§ 2511(2)(a)(ii), 2511(2), 2511(3), 2518(1), 2518(4), 2518(9)-(10), and 2519(3). Pub. L. No. 95-511 (1978). *See also infra* n.13.

[5] *See* 50 U.S.C. §§ 1804-05, 1806, 1809-10.

of Foreign Intelligence Surveillance Law, 72 Geo. Wash. L. Rev. 1306, 1312 (2004).

ARGUMENT

I. APPELLANTS' INVOCATION OF THE STATE SECRETS PRIVILEGE CONTRADICTS CONGRESS'S INTENT THAT COURTS REVIEW THE LEGALITY OF ELECTRONIC SURVEILLANCE CONDUCTED FOR NATIONAL SECURITY PURPOSES

The legislative history of FISA demonstrates that Congress intentionally gave the judiciary a central role in preventing Executive branch abuses in the context of electronic surveillance conducted for national security purposes. From the earliest hearings on legislative proposals, Congress assessed the practical and legal viability of judicial review over foreign intelligence surveillance. *See, e.g.,* Surveillance Practices and Procedures Act of 1973, S. 2820, 93rd Cong. (1973); Bill of Rights Procedures Act of 1974, S. 3440, 93rd Cong. (1974); Freedom From Surveillance Act of 1974, S. 4062, 93rd Cong. (1974). After extensive deliberation and debate, Congress concluded that the protection of civil liberties requires comprehensive judicial oversight of electronic surveillance conducted in the name of national security, as a check against documented overreaching by the Executive.

A. Congress Rejected Proposed Statutory Schemes Under Which the Judiciary Would Have Had Little Role in Assessing the Legality of Electronic Surveillance Conducted for Foreign Intelligence Purposes

By invoking the *Totten/Tenet* bar and the States Secret Privilege, Appellants effectively seek to revive the same argument that Congress flatly rejected almost thirty years ago—that the judiciary should have no meaningful role in reviewing the legality of electronic surveillance conducted for foreign intelligence purposes. In the course of FISA's legislative history, various House and Senate committees heard testimony arguing that courts are not capable of providing effective judicial review over foreign intelligence surveillance because of judges' alleged inexperience in foreign intelligence matters and the possibility of intelligence leaks. *See, e.g.*, H.R. Rep. No. 95-1283, at 25 (1978); *1974 S. Judiciary Comm. Hearings*, *supra* page 5, at 255. Along similar lines, some members of Congress suggested a statutory system that was functionally equivalent to the pre-FISA regime of un-checked Executive authority. *See, e.g., Foreign Intelligence Electronic Surveillance: Hearings on H.R. 5794, H.R. 9745, H.R. 7308, and H.R. 5632, The Foreign Intelligence Surveillance Act of 1977, Before the Subcomm. on Legis. of the H. Permanent Select Comm. on Intelligence*, 95th Cong. 3 (1978) (statement of Rep. McClory, introducing a competing bill which "retains with the

Executive—where it should be—the authority to approve national security foreign intelligence surveillance").

A strong majority in Congress rejected that position. As the House Intelligence Committee noted several months before FISA's passage:

> With all due respect to those views, the committee's conclusion ... is that a warrant requirement for electronic surveillance for foreign intelligence purposes will not pose unacceptable risks to national security interests and will remove any doubt as to the lawfulness of such surveillance. Moreover, there is no validity to the assertion that judges will somehow become involved under the bill in making foreign policy or foreign intelligence policy.

H.R. Rep. No. 95-1283, at 25. Senator Kennedy, who co-sponsored FISA, agreed, arguing that "[i]n order to remedy the abuses inherent in warrantless wiretapping a court order must be obtained before any wiretapping or bugging—even in the so-called 'national security' arena—can be permitted." *1974 S. Judiciary Comm. Hearings*, *supra* page 5, at 40.[6]

In the end, the legislation that Congress enacted reflects its judgment that the judiciary must play a central role in assessing the legality of electronic

[6] *See also* Senate Judiciary Committee Report, No. 94-1035, at 79 (1976) ("We believe that these same issues—secrecy and emergency, judicial competence and purpose—do not call for any different result in the case of foreign intelligence collection through electronic surveillance."); Foreign Intelligence Surveillance Act of 1977: Hearings Before the Subcomm. on Criminal Laws and Procedures of the Senate Comm. on the Judiciary 95th Cong., at 26 (1977) (Attorney General Bell asserting that "[t]he most leakproof branch of the Government is the judiciary . . . I have seen intelligence matters in the courts. . . I have great confidence in the courts," and Senator Orrin Hatch replying, "I do also").

surveillance conducted for foreign intelligence purposes. Congress provided for federal judicial review of government electronic surveillance initiatives both before the government may lawfully initiate surveillance, *see* 50 U.S.C. § 1804-5, and to determine the legality of surveillance after it has already been conducted, *see* 50 U.S.C. § 1806.

Appellants' attempt to quash the present litigation is therefore inconsistent with Congress's view of the importance of judicial review over electronic foreign intelligence surveillance. Indeed, Senator Mathias, Jr. declared at the time that "[t]he overriding significance" of FISA was "its requirement that an impartial magistrate outside the executive branch and the intelligence community must authorize electronic surveillance in foreign intelligence or national security cases." S. Rep. No. 94-1035, at 120 (1976) (describing an earlier version of the legislation that would become FISA). To permit Appellants' use of *Totten/Tenet* or the state secrets privilege would eliminate any judicial review of electronic surveillance conducted for foreign intelligence purposes, either before or after the fact of surveillance, and subvert Congress's clear intent to impose a check against Executive overreaching in a context historically fraught with civil liberties abuses.[7]

[7] It is important to note that at the time Congress was carefully drafting FISA, it was unthinkable that a President might completely ignore Congress's mandatory framework for conducting foreign intelligence gathering surveillance. When Senator Kennedy inquired of

B. Congress Crafted Carefully Balanced Procedures at 50 U.S.C. § 1806(f) By Which Federal Courts Are To Assess The Lawfulness of Surveillance After It Has Been Conducted

In FISA, Congress prescribed specific procedures to be used in the course of litigation concerning otherwise secret intelligence initiatives. In a deliberate effort to balance the need for openness necessary to protect civil liberties with the need for secrecy in foreign intelligence investigations, Congress limited the government's ability to withhold information related to such surveillance during litigation. As Appellees correctly argue, the statutory mechanism addressing the need for secrecy in litigation at 50 U.S.C. § 1806(f) effectively derogates the common law State Secrets doctrine and prevents the application of the *Totten/Tenet* bar. As *Amici Curiae* Professor Erwin Chemerinsky et al. explain, with FISA Congress has displaced the state secrets privilege where governmental electronic surveillance programs are challenged, and it is well within Congress's constitutional power to do so. *See* Br. of Erwin Chemerinsky et al. at Parts I(a) and I(b).

---

the sitting Attorney General about this specific issue, Attorney General Edward Levi responded, "I really cannot imagine a President, if this legislation is in effect, going outside the legislation for matters which are within the scope of this legislation." *Foreign Intelligence Surveillance Act of 1976: Hearings on S. 743, S. 1888 and S. 3197 Before the Subcomm. on Criminal Laws and Procedures of the S. Comm. on the Judiciary*, 94th Cong. 16 (1976).

FISA's § 1806(f) establishes that under certain circumstances, information that the Attorney General believes could "harm the national security of the United States" but that is "related to" government electronic surveillance must be subject to *in camera* and *ex parte* review by the district court. The Congressional committees responsible for §1806(f) envisioned that information related to surveillance would be disclosed to the subjects of that surveillance during litigation, absent a government assertion that disclosure would harm the national security. S. Rep. No. 95-701, at 63 (1978); *accord* S. Rep. No. 95-604(I), at 57. In light of this legislative solution to the policy problem of how—and whether—courts should consider sensitive national security information during litigation over the lawfulness of electronic surveillance, Appellants' attempted use of the *Totten/Tenet* bar and the state secrets privilege would subvert Congress's intent.

1. Congress Intended For § 1806(f) To Be The Exclusive Means To Address The Need For Secrecy In Litigation Over Electronic Surveillance Conducted For National Security Purposes

FISA reflects Congress's decision that, in general, information related to foreign intelligence surveillance should be disclosed to the courts and parties during litigation challenging Executive branch surveillance and private parties' cooperation. To account for the possibility that such disclosure may conflict

with national security concerns, Congress included a provision in § 1806(f) prescribing *in camera* and *ex parte* review of evidence in those circumstances. The legislative history shows that Congress intended for this procedure to be the exclusive means by which the Executive may assert the need for secrecy around information that might endanger the national security if publicized but is nevertheless relevant to litigation over electronic surveillance.

The Senate Intelligence Committee was particularly clear on this point. It noted that the procedures under which the may consider sensitive information, now codified at § 1806(f), may be "triggered by a government affidavit that disclosure or an adversary hearing would harm the national security of the United States." However, where "no such assertion is made the Committee envisions that mandatory disclosure of the application and order, and discretionary disclosure of other surveillance materials, would be available to the [aggrieved party]." S. Rep. No. 95-701, at 63; *accord* S. Rep. No. 95-604(I), at 57. This vision would be destroyed by Appellants' proposed use of the state secrets privilege in this case.

The Senate Judiciary Committee also articulated in its report that parties to litigation should not be allowed to skirt the § 1806(f) procedures by invoking other laws or jurisprudential doctrines:

> The Committee wishes to make clear that the procedures set out in [the subsection ultimately codified at § 1806(f)] apply whatever the underlying rule or statute referred to in [a party's] motion. This is necessary to prevent the carefully drawn procedures in [the same subsection] from being bypassed by the inventive litigant using a new statute, rule or judicial construction.

S. Rep. No. 95-604(I), at 57; *accord* S. Rep. No. 95-701, at 63; H.R. Rep. No. 95-1283, at 91. Indeed, the Committee signaled its intent that under § 1806(f), unlike the state secrets privilege, the Executive is required to cooperate with the court's *in camera* review. S. Rep. No. 95-604(I), at 57; *accord* S. Rep. No. 95-701, at 63 ("When the procedure is so triggered, however, the Government *must* make available to the court a copy of the court order and accompanying application upon which the surveillance was based." (emphasis added)). Congress repeatedly insisted that when the legality of surveillance is at issue, "it is this procedure 'notwithstanding any other law' that must be used to resolve the question." S. Rep. No. 95-604(I), at 57; *accord* S. Rep. No. 95-701, at 63; H.R. Rep. No. 95-1283, at 91.

The government's assertion that § 1806(f) is "not the exclusive means of addressing disputes involving classified surveillance activities" is incorrect. Intervenor United States of America's Reply in Supp. of Mot. to Dismiss at 20, *Hepting, et al., v. AT&T Corp., et al.* (N.D. Cal., No. C-06-0672-VRW). While it is true that *ex parte* and *in camera* review are triggered only if the

government claims a need for secrecy, those procedural protections are the full extent of the measures that Congress made available to protect the need for secrecy in litigation concerning electronic foreign intelligence surveillance.

2. The Legislative History Behind § 1806(f) Reveals A Careful And Deliberate Effort To Balance National Security Concerns Against The Rights Of Aggrieved Persons

The legislative history of FISA demonstrates that with § 1806(f), Congress sought to achieve a "fair and just balance between protection of national security and protection of personal liberties." S. Rep. No. 94-1035, at 9. Accordingly, Congress carefully considered each component of § 1806(f) for its potential impact on this balance and determined that it adequately protected national security interests. These provisions include *in camera* and *ex parte* review of evidence pertaining to the legality of surveillance in specific circumstances,[8] and discretionary or limited disclosure to aggrieved persons if necessary to make an accurate determination of the legality of the surveillance.

Congress specifically considered the adequacy of *in camera* and *ex parte* review in the event that the government files an affidavit attesting that

[8] These scenarios include: (1) when the government intends to use evidence against an aggrieved person; (2) if the aggrieved person moves to have the evidence suppressed; or (3) "whenever any motion or request is made by an aggrieved person ... 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 Act." 50 U.S.C. § 1806(f).

information "related to" electronic surveillance must be kept secret for national security reasons. *See* § 1806(f). The Senate Judiciary Committee reported that the provision "strik[es] a reasonable balance between an entirely *in camera* proceeding . . . and mandatory disclosure, which might occasionally result in the wholesale revelation of sensitive foreign intelligence information." S. Rep. No. 95-604(I), at 58. The House and Senate agreed, declaring in the Conference Report that "an *in camera* and *ex parte* proceeding is appropriate for determining the lawfulness of electronic surveillance[.]" H.R. Rep. No. 95-1720, at 32 (1978) (Conf. Rep.).

Congress also scrutinized the standards for disclosure of evidence to aggrieved persons in § 1806(f) to evaluate their impact on national security. Ultimately, all the relevant committees concluded that as a default rule, when there is a reasonable question as to the legality of the surveillance, disclosure to the aggrieved party is appropriate. *See* H.R. Rep. No. 95-1283, at 90 ("Whenever there is a *reasonable question of legality,* it is hoped that disclosure . . . *will be the usual practice*.") (emphasis added); S. Rep. No. 95-604(I), at 58 and S. Rep. No. 95-701, at 64 ("Thus, in some cases, the court will likely be able to determine the legality of the surveillance without any disclosure to the defendant [whereas i]n other cases, . . . the Committee contemplates that the

court will likely decide to order disclosure to the [aggrieved person].").[9] The committees also stated that after the Attorney General files a § 1806(f) affidavit, the appropriateness of disclosure is a "decision ... *for the Court to make*[.]" S. Rep. No. 95-701, at 64 (emphasis added); *accord* S. Rep. No. 95-604(I), at 58.

The House Conference Committee ultimately determined that "the standard for disclosure in the Senate bill adequately protects the rights of the aggrieved person, and that the provision for security measures and protective orders ensures adequate protection of national security interests." H.R. Rep. No. 95-1720, at 32 (Conf. Rep.). Congress's careful consideration of each component of these procedures demonstrates that § 1806(f) amounts to a reasoned legislative answer to the policy question of how the need for secrecy should be accommodated in litigation over foreign intelligence gathering.

3. Appellants' Assertion of The State Secrets Privilege and *Totten/Tenet* Bar Here Contradicts the Congressional Intent Behind § 1806(f)

Where Congress has created such detailed procedures by which the courts may assess the lawfulness of electronic surveillance conducted for national security purposes, it is extraordinary for Appellants to argue that review by the courts is inappropriate. Section 1806(f) and the two common law

[9] It also intended that "all orders regarding ... disclosure shall be final and binding ... against the government." H.R. Rep. No. 95-1720, at 32 (Conf. Rep.).

doctrines the government wishes to use here serve nearly identical functions; each provides for secrecy where the government seeks to protect from disclosure evidence that would allegedly threaten national security if revealed. *See Kasza v. Browner*, 133 F.3d 1159, 1166 (9th Cir. 1998); *see also, United States v. Reynolds*, 345 U.S. 1, 7-8 (1953). A critical difference, however, is that the *Totten/Tenet* bar and the state secrets privilege take account of a narrower range of interests; with § 1806(f), Congress intended not only to ensure secrecy where necessary, but also to ensure that citizens' civil liberties would be protected.

The government argues that because it has invoked the state secrets privilege, the Court may not balance the respective needs of the parties and instead may only assess whether disclosure would present a reasonable danger that national security would be harmed. Br. of Intervenor-Appellant United States of America at 16 (March 9, 2007). With § 1806(f), however, Congress crafted a procedure for *precisely* the purpose of balancing the need for national security with the rights of aggrieved persons. H.R. Rep. No. 95-1720, at 32 (Conf. Rep.). Appellants' assertion of the state secrets privilege disregards that intent and circumvents Congress's legislative determination to balance the need for secrecy in litigation over foreign-intelligence gathering electronic

surveillance initiatives with the need to preserve substantive rights and protect against abuses.

Appellants' assertion of the *Totten/Tenet* Bar[10] is even more at odds with the Congressional intent expressed in § 1806(f). Because this common law doctrine would preclude *any* judicial review, *Tenet*, 544 U.S. at 8, it is irreconcilable with Congress's prescription that a federal court may conduct post-surveillance review of the legality of electronic surveillance. The contention that suits such as this are not *justiciable* due to a "public policy forbid[ding] … disclosure of matters which the law itself regards as confidential," Br. of Intervenor-Appellant United States of America at 18 (March 9, 2007) (quoting *Totten*, 92 U.S. at 107), is without merit given that Congress has prescribed disclosure unless secrecy is required and has further prescribed precise means by which sensitive information should be handled during litigation.

If this Court were to sanction the government's use of the state secrets privilege or the *Totten/Tenet* Bar, it would allow the Executive to effect a rebalancing of national security and individual rights by avoiding the judicial review over foreign intelligence surveillance activities required by FISA both

[10] *Totten v. United States*, 92 U.S. 105 (1875); *Tenet v. Doe*, 544 U.S. 1 (2005).

before and after surveillance. As the House Permanent Select Committee on Intelligence remarked just before Congress passed FISA:

> the decision as to the standards governing when and how foreign intelligence electronic surveillances should be conducted is and should be a political decision, in the best sense of the term, because it involves the weighing of important public policy concerns—civil liberties and the national security. Such a political decision is one properly made by the political branches of Government together, not adopted by one branch on its own and with no regard for the other. Under our Constitution legislation is the embodiment of just such political decisions.

H.R. Rep. No. 95-1283, at 21-22. Where Congress has made a considered policy choice and prescribed not just the availability of a cause of action but also the precise procedures by which litigation should transpire, common law doctrines cannot be used to circumvent this legislative judgment. *See* Br. of Prof. Erwin Chemerinsky et al. at Parts I(a)(1) and I(b).

II. THE LEGISLATIVE HISTORY OF FISA'S CIVIL CAUSE OF ACTION DEMONSTRATES THAT CONGRESS CONSIDERED AND ACCOUNTED FOR THE NEED FOR SECRECY IN LITIGATION OVER ELECTRONIC SURVEILLANCE CONDUCTED FOR NATIONAL SECURITY PURPOSES

Like the legislative history behind § 1806(f), the legislative history behind the civil cause of action against private parties for violations of FISA[11]

[11] *See* 50 U.S.C. § 1810; 18 U.S.C. §§ 2520, 2511(2)(a)(ii); *infra* n.14.

further confirms that Appellants' assertions of the state secrets privilege and the *Totten/Tenet* bar to litigation are inconsistent with Congress's legislative intent.

FISA amended 18 U.S.C. § 2511(2)(a)(ii) (1970) to specify that a "communications common carrier"[12] must receive either a court order requiring assistance from the common carrier or a certification that the prospective electronic surveillance is legal before it may help the government to monitor customer communications. FISA § 201(a).[13] As a result, if a telephone company assists the government in conducting surveillance without a § 2511 court order or certification, it is explicitly liable for damages under 18 U.S.C. § 2520.[14] The legislative history of these provisions indicates that this additional requirement and the resulting exposure to liability for phone

---

[12] Congress amended § 2511(2)(a)(ii) in 1986, replacing the phrase "communication common carriers" with "providers of wire or electronic communication service." *See, e.g.*, Electronic Communications Privacy Act of 1986 § 101(c)(6)(A).

[13] The United States suggests that § 2511(2)(a)(ii) is part of Title III rather than FISA. Br. of Intervenor-Appellant United States of America at Addendum at 3A-4A (March 9, 2007). While it is true that 18 U.S.C. § 2511(2)(a)(ii) predates FISA, (*see* District of Columbia Court Reform and Criminal Procedure Act of 1970, Pub. L. No. 91-358, 77 Stat. 478 § 211(a)(2) (1970)), FISA introduced substantial revisions to that section, including the requirement for a court order or a certification. *See also, infra* n.17.

[14] Damages for violations of 18 U.S.C. § 2511(2)(a)(ii) are also available under 50 U.S.C. § 1810—as § 1810 provides a cause of action for violations of § 1809, which makes it illegal to "engage[] in electronic surveillance under color of law except as authorized by statute." *See* § 1809(a)(1). Because 18 U.S.C. § 2511(2)(a)(ii) set the bounds of lawful electronic surveillance by "common communication carriers" (now "providers of wire or electronic communication service," *see supra* n.12), surveillance outside those bounds was and remains *unauthorized* by statute and therefore subject to liability under 50 U.S.C. § 1810.

companies that do not meet it reflect Congress's effort to balance the need for effective and discreet foreign intelligence with the need for judicial review of surveillance activity. The imperative for secrecy around evidence of electronic foreign intelligence surveillance is therefore already accounted for in FISA's provision of liability for companies like AT&T.

FISA's court order or certification requirement originated in S. 4062, "The Freedom from Surveillance Act of 1974." In October 1974, Senator Kennedy presented to the Subcommittee of the Senate Judiciary Committee an analysis of how S. 4062 would change prevailing laws. He explained:

> Section 4 of the Freedom from Surveillance Act of 1974 would amend 18 U.S.C. § 2511(2)(a)(ii) to require communications carriers to obtain a certified copy of the court order[15] authorizing or approving the interception before rendering assistance to those seeking to intercept wire or oral communications. . . Failure to comply with [this] requirement[] would subject those responsible to criminal and/or civil liability under the provisions of 18 U.S.C. §§ 2510-2520.[16] The purpose of these amendments is to limit the availability of assistance from the communications carrier to those instances where interception of wire or oral communications is to

[15] S.4062 required a "duly certified copy" of the relevant court order before permitting communication carriers to cooperate with surveillance efforts. S.4062 § 4 (1974). FISA, as codified at 18 U.S.C. § 2511(2)(a)(ii), ultimately permits such cooperation upon receipt of either a court order or certification from another appropriate authority, such as the Attorney General. *See* 18 U.S.C. §§ 2511(2)(a)(ii), 2518(7). The certification alternative was intended to only be used in situations where a court order was not required, such as surveillance conducted pursuant to the emergency provisions. *See infra p.* 27-28.

[16] At the time, these were the sole statutory provisions governing the legality of electronic surveillance. *See 1974 S. Judiciary Comm. Hearings*, *supra* page 5, at 33-38. Ultimately, Congress would codify much—though not all—of FISA at 50 U.S.C. § 1801 *et seq*.

> be conducted under judicial supervision and to provide litigants with a source of evidence of interception.

1974 S. Judiciary Comm. Hearings, *supra* page 5, at 33-34. As this passage and others indicate, the prospect of litigation over electronic surveillance—and specifically over electronic surveillance "based on national security grounds," in Senator Kennedy's words—was a key driver of the certification requirement. *See also* S. Rep. No. 95-604(I), at 62 ("Violation of this subsection by a carrier or its representative will render the carrier liable for the civil damages provided for in Section 2520."); S. Rep. 94-1035 at 54.

Congress ultimately enacted these proposed provisions largely unaltered. FISA § 201(a) (amending 18 U.S.C. § 2511(2)(a)(ii)). The House Permanent Select Committee on Intelligence reported that:

> [r]equiring the court order or certification to be presented [to telephone companies] before the assistance is rendered serves two purposes. It places an *additional obstacle in the path of unauthorized surveillance* activity, and, coupled with the provision relieving the third party from liability if the order or certification is complied with, it provides full protection to such third parties.… The committee provision is intended to hold harmless the phone company and others *so long as the assistance is in accordance with the terms of the order or certification… "*

H.R. Rep. No. 95-1283, at 99 (emphasis added). The House Committee thus saw the requirement as both protection against illegal surveillance and a means

of clarifying the circumstances under which phone companies would be liable for cooperating with government intelligence gathering initiatives.

Although § 2511(2)(a)(ii) permits cooperation if the private party has received either a court order or certification, the legislative history demonstrates that Congress did not consider the two to be available in exactly the same circumstances. As the House Intelligence Committee noted:

> [w]here a court order is required to initiate a surveillance, a copy of the order must be provided to the party rendering assistance. Where a court order is not required, a copy of the relevant Attorney General certificate must be provided.

H.R. Rep. No. 95-1283, at 99. The Senate Intelligence and Judiciary Committees offered a similar clarification, noting that "before the carrier may provide such information or assistance ... the Government agent must furnish the carrier with an order signed by the court ... if an order has been acquired." S. Rep. No. 95-604(I), at 62; *accord* S. Rep. No. 95-701, at 69. The certification, by comparison, is only appropriate when "the surveillance is being conducted pursuant to the provisions of section 2518(7) ... or [50 U.S.C. § 1805(f)] [authorizing surveillance in emergency situations]." S. Rep. No. 95-604(I), at 62; *accord* S. Rep. No. 95-701, at 69. Given the difference envisioned between court orders and certifications, a certification may still be insufficient to satisfy the requirements of § 2511(2)(a)(ii) in circumstances

where the surveillance exceeds those permitted by the emergency provisions, or where emergency surveillance is not permitted.

Furthermore, Congress was clearly aware that sensitive information would be at issue in litigation over the legality of cooperation between telephone companies and government surveillance programs under § 2511(2)(a)(ii).[17] To address this possibility, Congress specifically forbade common carriers from disclosing information relating to these surveillance efforts except as "required by legal process." FISA § 201(a) (amending 18 U.S.C. § 2511(2)(a)(ii)). However, in the event that legal process does require the carrier to disclose such information, the carrier must first give notice to the Attorney General or another authority. *Id.* The House Intelligence Committee reported that this notice requirement was designed to allow the government to assert the need for secrecy, consistent with the statutory framework Congress envisioned. H.R. Rep. No. 95-1283, at 99 n.53.[18]

When read in conjunction with 50 U.S.C. § 1806(f), the notice provision in § 2511(2)(a)(ii) is further evidence that Congress fully considered and

[17] The House Intelligence Committee explicitly articulated its intent to "extend [the] scope" of the §2511(2)(a)(ii) court order or certification requirement "to cover foreign intelligence electronic surveillance." H.R. Rep. No. 95-1283, at 98. *See* 50 U.S.C. § 1801(e) (2006) (defining "foreign intelligence," unchanged from the 1978 version).

[18] The notice requirement had its origins in the House version of the bill. *See* H.R. Rep. No. 95-1720, at 34-35 (Conf. Rep.)

addressed the need for secrecy, even in litigation involving surveillance efforts aided by common carriers, within the statutory scheme of FISA. Given that § 1806(f) embodies a careful balance between the need for secrecy and rights of aggrieved persons, *see supra* Part I.B.2, the notice provision in § 2511(2)(a)(ii) essentially provides a means by which the government may invoke § 1806(f) in a suit against private parties.

Congress's decision to establish civil actions arising when telephone companies unlawfully cooperate with government surveillance programs is comprehensive, straightforward and unambiguous. Appellants argue, however, that because "[t]he critical premise of the complaint is that AT&T has been collaborating with NSA in a ... classified surveillance program," the litigation should be halted—since "lawsuits premised on alleged espionage agreements are altogether forbidden." Br. of Intervenor-Appellant United States of America at 18 (March 9, 2007) (internal quotations omitted). As the legislative history reveals, though, the primary purpose behind the certification requirement of § 2511(2)(a)(ii) is to dictate precisely when and under what circumstances such collaboration between AT&T and the government is permissible. By seeking dismissal under the state secrets privilege and the *Totten/Tenet* bar, Appellants effectively assert that Congress either has not regulated or may not regulate communication service providers in this context.

This position belies the plain language of the statute and its legislative history, and it ignores the gross abuses of civil liberties that inspired FISA's passage along with the constitutional principle that Congress can and must use its legislative powers to act as a check against the Executive branch.

CONCLUSION

For the reasons set forth above, People For the American Way Foundation respectfully urges this Court to affirm the district court's decision.

DATED: May 2, 2007

SAMUELSON LAW, TECHNOLOGY & PUBLIC POLICY CLINIC
UNIVERSITY OF CALIFORNIA—BERKELEY SCHOOL OF LAW (BOALT HALL)

By:

_____

JACK I. LERNER (220661)
DEIRDRE K. MULLIGAN (218804)
396 Simon Hall
Berkeley, CA 94720-7200
Telephone: (510) 643-7515
Facsimile: (510) 643-4625

Counsel for *Amicus Curiae*

JUDITH E. SCHAEFFER
PEOPLE FOR THE AMERICAN WAY FOUNDATION
2000 M Street, NW, Suite 400
Washington, DC 20036
Telephone: (202) 467-4999
Facsimile: (202) 293-2672

CERTIFICATE OF COMPLIANCE

I certify that the foregoing Brief for *Amicus Curiae* People For The American Way Foundation has a typeface of 14 points or more and complies with the 7,000 word type-volume limitation of Fed. R. App. P. 29(d) and 32(a)(7)(B) in that it contains 6,924 words, including both text and footnotes and excluding the table of contents, table of authorities, certificates of counsel, and corporate disclosure statement. The number of words was determined using the Word Count function of Microsoft Office Word 2003.

DATED: May 2, 2007

By:

_____

SAMUELSON LAW, TECHNOLOGY
& PUBLIC POLICY CLINIC
UNIVERSITY OF CALIFORNIA—BERKELEY
SCHOOL OF LAW (BOALT HALL)
JACK I. LERNER (220661)
DEIRDRE K. MULLIGAN (218804)
396 Simon Hall
Berkeley, CA 94720-7200
Telephone: (510) 642-7515
Facsimile: (510) 643-4625

Counsel for *Amicus Curiae*

CERTIFICATE OF SERVICE

I, Rebecca Henshaw, certify and declare as follows:

I am over the age of 18 years, not a party to this cause, and employed in the county where the mailing took place. My business address is Center for Clinical Education, University of California at Berkeley School of Law (Boalt Hall), 396 Simon Hall, Berkeley, CA 94720-7200, which is located in Alameda County.

On May 2, 2007, I served the following document(s):

BRIEF AMICUS CURIAE OF PEOPLE FOR THE AMERICAN WAY FOUNDATION IN SUPPORT OF PLAINTIFFS-APPELLEES

by placing a true copy thereof in a sealed envelope and served to each party herein by delivery via **FEDERAL EXPRESS** mail to:

Peter D. Keisler
Carl J. Nichols
Anthony J. Coppolino
Andrew H. Tannenbaum
Joseph Hunt
U.S. Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Avenue N.W.
Room 6102
Washington, D.C. 20001
(202) 514-4782 (tel.)
(202) 616-8470 (fax)

Bruce A. Ericson
Kevin M. Fong
Marc H. Axelbaum
Jacob R. Sorensen
Pillsbury Winthrop Shaw Pittman LLP
50 Fremont Street
San Francisco, CA 94105
(415) 983-1000 (tel.)
(415) 983-1200 (fax)

Paul D. Clement
Gregory G. Garre
Daryl Joseffer
Office of the Solicitor General
950 Pennsylvania Avenue NW
Suite 5143
Washington, D.C. 20530-2201
(202) 514-2201 (tel.)
(202) 514-3648 (fax)

Michael K. Kellogg
Sean A. Lev
Kellogg, Huber, Hansen, Todd,
Evans & Figel, P.L.L.C.
1615 M. Street, N.W., Suite 400
Washington, D.C. 20036
(202) 326-7900 (tel.)
(202) 326-7999 (fax)

Douglas N. Letter
Thomas M. Bondy
Anthony A. Yang
U.S. Department of Justice
Civil Division, Appellate Staff
950 Pennsylvania Avenue N.W.
Room 7513
Washington, D.C. 20530-0001
(202) 514-3602 (tel.)
(202) 514-8151(fax)

Bradford Berenson
David Lawson
Edward R. McNicholas
Sidley Austin LLP
1501 K. Street, NW
Washington D.C. 20005
(202) 736-8000 (tel.)
(202) 736-8711 (fax)

Cindy Cohn
Lee Tien
Kurt Opsahl
Kevin S. Bankston
James S. Tyre
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110
(415) 436-9333 (tel.)
(415) 436-9993 (fax)

Robert D. Fram
E. Joshua Rosenkranz
Michael M. Markman
Ethan C. Glass
Samuel F. Ernst
Nathan E. Shafroth
Elena M. DiMuzio
Heller Ehrman LLP
333 Bush Street
San Francisco, CA 94104
(415) 772-6000 (tel.)
(415) 772-6268 (fax)

I also submitted an original and 15 copies of the above stated document by **FEDERAL EXPRESS** to the 9th Circuit Court of Appeals at the following address:

Office of the Clerk
U.S. Court of Appeals
95 Seventh Street
San Francisco, CA 94103-1526

Executed on May 2, 2007, at Berkeley, California. I declare under penalty of perjury under the laws of the United States of America that the above is true and correct.

_____
Rebecca Henshaw