

Nos. 06-17132, 06-17137

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

TASH HEPTING, et al., Plaintiffs-Appellees.

v.

AT&T CORP., Defendant-Appellant, and

UNITED STATES OF AMERICA, Intervenor and Appellant.

ON 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 OF *AMICI CURIAE* NATIONAL ASSOCIATION FOR THE
ADVANCEMENT OF COLORED PEOPLE, AMERICAN-ARAB ANTI-
DISCRIMINATION COMMITTEE, ASIAN AMERICAN LEGAL
DEFENSE AND EDUCATION FUND, JAPANESE AMERICAN
CITIZENS LEAGUE, THE LEAGUE OF UNITED LATIN AMERICAN
CITIZENS, AND UNITED FOR PEACE AND JUSTICE
SUPPORTING PLAINTIFFS – APPELLEES URGING AFFIRMANCE

Jonathan Hafetz
Aziz Z. Huq
Frederick A.O. Schwarz, Jr.
BRENNAN CENTER FOR JUSTICE
AT NYU SCHOOL OF LAW
161 Ave. of the Americas – 12th Floor
New York, New York 10013
Telephone: (212) 998-6730
Facsimile: (212) 995-4550

Marc Van Der Hout
Beth Feinberg
VAN DER HOUT, BRIGAGLIANO
& NIGHTINGALE, LLP
180 Sutter Street, Fifth Floor
San Francisco, California 94104-4029
Telephone: (415) 981-3000
Facsimile: (415) 981-3003

TABLE OF CONTENTS

	<u>Page</u>
INTEREST OF <i>AMICI CURIAE</i>	1
INTRODUCTION AND SUMMARY OF ARGUMENT	4
ARGUMENT	7
I. THE CHURCH COMMITTEE REVEALED THAT FOR DECADES INTELLIGENCE AGENCIES SECRETLY SPIED ON LAW-ABIDING AMERICANS IN THE NAME OF NATIONAL SECURITY.	7
II. THE CHURCH COMMITTEE DEMONSTRATED THAT THE SECRECY SURROUNDING NSA SURVEILLANCE WAS DESIGNED TO PROTECT EXECUTIVE MALFEASANCE AND NOT NATIONAL SECURITY.	11
A. The Secrecy That Surrounded the NSA Served To Shield It From Oversight And Immunize Its Operations From Legal Sanction, Not To Protect National Security.	12
B. The Church Committee’s Public Disclosure Of Allegedly Sensitive Information Concerning Telegraph Companies’ Involvement In Operation Shamrock Led To Greater Oversight Of NSA Surveillance Without Harming National Security.	17
III. FISA CODIFIED THE CHURCH COMMITTEE’S RECOMMENDATIONS TO REQUIRE THAT FEDERAL COURTS REVIEW THE LEGALITY OF SURVEILLANCE PROGRAMS, EXECUTIVE CLAIMS OF STATE SECRETS PRIVILEGE NOTWITHSTANDING.....	20
A. FISA Requires That The Federal Judiciary Authorize and Review All Executive Electronic Surveillance, Both <i>Ex Ante</i> and <i>Ex Post</i>	21

TABLE OF CONTENTS
(continued)

	<u>Page</u>
B. FISA Requires That Federal Courts Exercise Oversight of Executive Surveillance, Regardless of Executive Invocations of State Secrecy Privileges.	23
CONCLUSION.....	26
CERTIFICATE OF COMPLIANCE	

TABLE OF AUTHORITIES

Page

Federal Cases

<i>Berger v. New York</i> , 388 U.S. 41 (1967)	8
<i>Fairfax's Devisee v. Hunter's Lessee</i> , 11 U.S. (7 Cranch) 603 (1812).....	24
<i>Hamdan v. Rumsfeld</i> , 126 S. Ct. 2749 (2006)	25
<i>Hepting v. AT&T</i> , 439 F. Supp. 2d 974 (N.D. Cal. 2006)	4, 5, 24
<i>In re United States</i> , 872 F.2d 472 (D.C. Cir. 1989).....	24
<i>Nardone v. United States</i> , 308 U.S. 338 (1939)	8
<i>Youngstown Sheet & Tube Co. v. Sawyer</i> , 343 U.S. 579 (1952).....	25

Federal Statutes

Foreign Intelligence Surveillance Act, Pub. L. 95-511, Title I, 92 Stat. 1796 (Oct. 25, 1978).....	4
Intelligence Authorization Act for FY1993, Pub. L. No. 102-496 (1992)...	12
USA PATRIOT Act, Pub. L. No. 107-56, § 218, 115 Stat. 272 (2001).....	25
18 U.S.C. § 2511	22
18 U.S.C. § 2520.....	22
18 U.S.C. § 2707	22
47 U.S.C. § 605(a)	8
47 U.S.C. § 605(e)(3)(A)	23
50 U.S.C. § 401	13

TABLE OF AUTHORITIES
(continued)

	<u>Page</u>
50 U.S.C. § 1804(a)(7)(B)	25
50 U.S.C. § 1805(a)(3).....	21
50 U.S.C. § 1806(f).....	24
50 U.S.C. § 1809.....	22
50 U.S.C. § 1810.....	22

Other Authorities

Exec. Order No. 12,333	13
S. Rep. No. 95-604 (I), <i>reprinted in</i> 1978 U.S.C.C.A.N. 3904	20, 21, 22
Senate Select Comm. to Study Governmental Operations with Respect to Intelligence Activities and the Rights of Americans (Book II), S. Rep. No. 94-755 (1976).....	<i>passim</i>
Senate 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 (1976)	<i>passim</i>
James Bamford, <i>The Puzzle Palace</i> (1983)	14, 15
Lowell Bergman et al., <i>Spy Agency Data After Sept. 11 Led F.B.I. to Dead Ends</i> , N.Y. Times (Jan. 17, 2006)	15
Francis Biddle, <i>In Brief Authority</i> (1962).....	11
James G. Hudec, <i>Unlucky Shamrock – The View From the Other Side</i> , Studies in Intelligence, (Winter/Spring 2001), <i>available at</i> https://www.cia.gov/csi/studies/winter_spring01/article12.pdf	19

TABLE OF AUTHORITIES

(continued)

	<u>Page</u>
Loch K. Johnson, <i>A Season of Inquiry: The Senate Intelligence Investigation</i> (1985).....	17, 18
Loch K. Johnson, <i>America's Secret Power: The CIA in a Democratic Society</i> (1989).....	13, 15
Lawrence D. Sloan, <i>Echelon and the Legal Restraints on Signals Intelligence: A Need for Reevaluation</i> , 50 Duke L.J. 1467 (2001).....	13
L. Britt Snider, <i>Unlucky Shamrock: Recollections From the Church Committee's Investigation of the NSA</i> , Studies in Intelligence (Winter 1999-2000), available at https://www.cia.gov/csi/studies/winter99-00/art4.html	18, 19
Athan Theoharis, <i>Spying on Americans: Political Surveillance From Hoover To The Huston Plan</i> (1978).....	13, 14, 15
Mark Tushnet, <i>Making Civil Rights Law: Thurgood Marshall and the Supreme Court, 1931-1961</i> (1994).....	10

INTEREST OF *AMICI CURIAE*¹

Amici curiae number among the most respected and long-established civil rights organizations in the United States.

The National Association for the Advancement of Colored People (“NAACP”) is a non-profit membership corporation originally chartered by the State of New York in 1909. The Nation’s oldest and largest civil rights organization, the NAACP has more than 500,000 members and 2,200 units in the United States and overseas.

The American-Arab Anti-Discrimination Committee (“ADC”) is a non-profit, non-partisan civil rights organization committed to defending the rights of people of Arab descent and promoting their rich cultural heritage. Founded in 1980, ADC is the largest Arab-American grassroots civil rights organization in the United States, with 38 chapters nationwide and members in all 50 states.

The Asian American Legal Defense and Education Fund (“AALDEF”), founded in 1974, is a non-profit organization based in New York City devoted to defending the civil rights of Asian Americans. AALDEF is concerned that the government’s reliance on vague and

¹ *Amici* file this brief with the consent of the parties.

unchecked war powers is the same purported basis that led to the unlawful internment of Japanese during World War II.

The Japanese American Citizens League (“JACL”) was founded in 1929. JACL is the nation’s oldest and largest Asian American non-profit, non-partisan organization, and is committed to upholding the civil rights of Americans of Japanese ancestry.

The League of United Latin American Citizens (“LULAC”), a non-profit membership organization chartered originally by the State of Texas in 1929, is the oldest and largest Latino civil rights organization in the United States. LULAC advances the economic condition, educational attainment, political influence, health, and civil rights of Hispanic Americans through community based programs operating at more than 700 LULAC councils nationwide.

United for Peace and Justice, with more than 1,400 member groups, is the nation’s largest antiwar coalition coordinating efforts in opposition to the U.S. war on Iraq. Since October 2002, United for Peace and Justice has supported hundreds of local protests and several of the largest protests against the war: three in New York City, on February 15, 2003, August 29, 2004, and April 29, 2006; and two in Washington, D.C., on September 24, 2005 and January 27, 2007.

Amici curiae civil rights organizations have long devoted substantial effort and resources to public advocacy on issues of concern to their members, advocacy often at odds with official government positions. Their First Amendment activities in consequence have historically been the target of clandestine surveillance by executive branch agencies. Corrosive and unconstitutional intrusions on the privacy of civil rights organizations and others who expressed then-unpopular views have muffled important voices in our Nation's struggle for Equal Justice Under Law. Such intrusion on protected speech and advocacy prompted Congress to involve the federal courts in the oversight of surveillance.

Amici's historical experience with unchecked domestic surveillance and excessive deference to executive claims of state secrecy has direct relevance to this appeal. The history recounted here properly informs the Court's analysis of the state secrets doctrine by highlighting the need for external scrutiny of domestic surveillance programs and showing that executive secrecy claims ought to be treated with caution and skepticism. In the past, it has been abuse, not needed intelligence activity, that the executive has hid from public sight.

INTRODUCTION AND SUMMARY OF ARGUMENT

Meaningful oversight of warrantless electronic surveillance trumps unquestioned deference to executive determinations of state secrecy. This simple axiom is the legacy of America's experience with domestic surveillance during the Cold War. It remains the standard governing the case before this Court.

The investigation of the United States Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities ("the Church Committee") into the history of secret warrantless surveillance led Congress to codify the above axiom in the Foreign Intelligence Surveillance Act ("FISA"), Pub. L. No. 95-511, Title I, 92 Stat. 1796 (Oct. 25, 1978). The history leading to FISA's enactment bears directly on the issues now before this Court.

In January 2006, customers of telecommunications giant AT&T brought suit against the company, claiming that AT&T was unlawfully assisting the National Security Agency ("NSA") in a domestic surveillance program, secretly authorized by the President to intercept Americans' communications without warrants. *Hepting v. AT&T*, 439 F. Supp. 2d 974, 979 (N.D. Cal. 2006). The government moved to intervene and sought dismissal, claiming the very existence of this lawsuit would expose sensitive

state secrets. *Id.* The district court denied the motion, holding that the state secrets doctrine did not justify dismissal. *Id.* at 980.

On appeal, the government and AT&T argue that the district court erred in its analysis of the state secrets doctrine and overstepped its institutional bounds by second-guessing an executive determination of what evidence or issues constitute a state secret. The government (Br. at 23) asserts that the district court “had no proper basis . . . for disagreeing with the assessments . . . from the Nation’s top-level intelligence officials.”

These claims should be rejected. The history of electronic surveillance in the United States that *amici* present here demonstrates three reasons why untrammelled deference to the executive is unwarranted. First, a lack of oversight during the Cold War allowed intelligence agencies to invoke “national security” as justification to spy on the constitutionally protected activity of an ever-widening group of innocent individuals and domestic civil rights organizations. Second, the executive branch kept Cold War intelligence operations secret to hide abuses of surveillance powers from Congress and the courts, not to protect national security information. The Church Committee’s exposure of domestic surveillance, over the executive’s objections, showed, first, that the American public can know details of surveillance at home without jeopardizing national security and,

second, that public scrutiny is vital to accountability. Finally, Congress enacted FISA with this history of abuse in mind, designing the legislation to strike a balance between oversight and secrecy that requires federal courts to look past rote executive invocation of state secrecy to determine the legality of warrantless surveillance.

In short, history warns against judicial deference to the executive claims of state secrecy invoked here. Rather, it shows the ability of and need for federal courts to subject secrecy claims to searching independent review. History demonstrates the danger of dismissing a suit challenging the legality of a warrantless wiretapping program based upon “state secrets,” a doctrine fundamentally at odds with the findings of the Church Committee and the statutory scheme in FISA enacted in response to those findings.

ARGUMENT

I. THE CHURCH COMMITTEE REVEALED THAT FOR DECADES INTELLIGENCE AGENCIES SECRETLY SPIED ON LAW-ABIDING AMERICANS IN THE NAME OF NATIONAL SECURITY.

From the 1930s to the 1970s, intelligence agencies under Democratic and Republican administrations spied on American citizens without warrants or judicial authorization. *See* Senate Select Comm. to Study Governmental Operations with Respect to Intelligence Activities and the Rights of Americans (Book II), S. Rep. No. 94-755, at 12 (1976) (“Church Committee Book II”). Most alarmingly, this surveillance frequently targeted individuals engaged in constitutionally protected political speech, including wholly-legitimate political dissent and civil rights activities. *Id.* at 213-214; *see also* Senate 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 4-5 (1976) (“Church Committee Book III”). As the Church Committee explained, the use of warrantless electronic surveillance for unconstitutional ends was enabled by a lack of oversight of intelligence activities and by application of an overbroad label of “national security.”

Congress attempted to restrain the executive’s ability to intrude on private communications as early as the 1930s. But, like today’s executive,

the Democratic Administrations of that day evaded the law and spied on Americans without warrants. Although the Federal Communications Act of 1934 made it unlawful to intercept and divulge such communications, 47 U.S.C. § 605(a), the Attorney General and his successors interpreted the 1934 Act to permit wiretapping as long as no information passed outside the government, Church Committee Book II, *supra*, at 36; *cf. Nardone v. United States*, 308 U.S. 338 (1939) (interpreting the Federal Communication Act of 1934 to bar both direct and indirect use of telephonic intercept evidence). This interpretation eliminated any external check on the executive branch's power to eavesdrop on even the most intimate conversations by dispensing with any requirement that government justify its suspicions. *Cf. Berger v. New York*, 388 U.S. 41. 63 (1967) ("Few threats to liberty exist which are greater than that posed by the use of eavesdropping devices").

Most consequent surveillance focused initially on the potential agents of foreign, totalitarian powers. Church Committee Book II, *supra*, at 21. Yet, over time there was a "steady increase in the government's capability and willingness to pry into, and even disrupt, the political activities and personal lives of the people." *Id.* Before long, intelligence activity also targeted domestic groups advocating social justice in America. Civil rights organizations became targets "without regard for the consequences to

American liberties.” *Id.* at 22. *Amici* NAACP, for example, was investigated for more than twenty-five years because the government believed that the organization might have once “had connections with” the Communist Party. *Id.* at 8. During that time, the government gathered extensive inside information about NAACP lobbying and advocacy efforts via electronic surveillance, *id.* at 232, while the FBI shared extensive reports on the NAACP with military intelligence, *id.* at 81 n.350. Other organizations targeted by warrantless surveillance included the Southern Christian Leadership Conference, the Congress on Racial Equality, the Student Nonviolent Coordinating Committee, the Urban League, and the Anti-Defamation League of B’nai B’rith. *Id.* at 105, 167. Individuals targeted by warrantless surveillance included civil rights leaders such as Dr. Martin Luther King, Jr., Coretta King, Julian Bond, and James Farmer. *Id.* at 81, 174.

Ever-widening illegal surveillance of wholly legitimate civil rights activity was framed in terms of national security. Without clear legal boundaries, intelligence personnel erred towards excess, hence viewing the struggle for racial equality through a Cold War prism as a threat to the nation’s safety. During the Civil Rights movement, for example, the government claimed that surveillance of Dr. King and members of the

NAACP was necessary to thwart communist subversion. See Mark Tushnet, *Making Civil Rights Law: Thurgood Marshall and the Supreme Court, 1931-1961*, at 295 (1994). Intelligence agencies justified their surveillance of these organizations and individuals by reflexively evoking labels of “national security,” “domestic security,” “subversive activities,” and “foreign intelligence.” Church Committee Book II, *supra*, at 205, 208.

The Church Committee pinpointed two dynamics central to the widening scope of Cold War domestic surveillance. The first was the tendency of unchecked, warrantless spying to target wholly innocent, constitutionally-protected political expression. Unchecked surveillance activity, the Committee concluded, inevitably “exceed[s] the restraints on the exercise of governmental power which are imposed by our country’s Constitution, laws, and traditions.” *Id.* at 2. The second was careless use by executive agencies of broad, amorphous labels such as “national security” and “subversion”:

[A]pplication of vague and elastic standards for wiretapping and bugging has resulted in electronic surveillances which, by any objective measure, were improper and seriously infringed the Fourth Amendment rights of both the targets and those with whom the targets communicated.

Church Committee Book III, *supra*, at 332. The danger of labels was not new. Reflecting on his World War II experience, former Attorney General

Francis Biddle noted with regret “the power of suggestion which a mystic cliché like ‘military necessity’ can exercise on human beings.” Francis Biddle, *In Brief Authority* 226 (1962). These two dynamics reinforced each other, allowing intelligence agencies to violate the constitutional rights of thousand of innocent Americans: “[T]he imprecision and manipulation of the[se] . . . labels, coupled with the absence of any outside scrutiny, has led to [their] improper use against American citizens who posed no criminal or national security threat to the country.” Church Committee Book II, *supra*, at 205.

II. THE CHURCH COMMITTEE DEMONSTRATED THAT THE SECRECY SURROUNDING NSA SURVEILLANCE WAS DESIGNED TO PROTECT EXECUTIVE MALFEASANCE AND NOT NATIONAL SECURITY.

Similar problems pervade the NSA’s history, which was in effect shrouded by secrecy until the Church Committee’s inquiry. The Church Committee’s investigation of the history and development of NSA surveillance programs proved that this secrecy was not necessary to protect national security interests. Rather, the Church Committee revealed, secrecy served only to shield the NSA and the telecommunications companies that participated in its programs from congressional and judicial oversight of illegal surveillance activities. The Committee’s decision to air these secrets to public scrutiny against the executive’s wishes demonstrates that oversight

and sometimes exposure of “state secrets” concerning warrantless domestic surveillance are necessary for the protection of constitutional freedoms and can occur without jeopardizing national security.

A. The Secrecy That Surrounded the NSA Served To Shield It From Oversight And Immunize Its Operations From Legal Sanction, Not To Protect National Security.

“Abuse thrives on secrecy,” the Church Committee concluded based upon its lengthy and thorough investigation of the NSA. Church Committee Book II, *supra*, at 292. The Committee explained that, while national security may justify nondisclosure of “names of intelligence agents or the technological details of collections of methods,” executive secrecy easily comes unmoored from national security goals, serving more often to hide executive malfeasance or prevent legal sanction. *Id.*

The NSA was cloaked in secrecy from its very beginning. In October 1952, President Harry S. Truman created the NSA within the Department of Defense by secret directive to marshal the Nation’s electronic surveillance resources for the Cold War. Church Committee Book III, *supra*, at 736. Until 1992, the agency operated without a legislative charter, *cf.* Intelligence Authorization Act for FY1993, Pub. L. No. 102-496, § 705 (1992), and, as late as 1981, no publicly available executive order limited the NSA’s power or set forth its responsibilities, *cf.* Exec. Order No. 12,333, § 1.12(b),

reprinted in 50 U.S.C. § 401; Lawrence D. Sloan, *Echelon and the Legal Restraints on Signals Intelligence: A Need for Reevaluation*, 50 Duke L.J. 1467, 1497-99 (2001) (describing E.O. 12,333).

Throughout most of the Cold War, secrecy allowed the NSA to conduct surveillance entirely without statutory or judicial check. Unrestrained by any other branch of government, the NSA grew “into a vast mechanical octopus, reaching sensitive tentacles into every continent in search of information on the intentions and capabilities of other nations.” Loch K. Johnson, *America’s Secret Power: The CIA in a Democratic Society* 52 (1989). Devoid of the external checks needed to prevent abuse of surveillance powers, the NSA inevitably turned its “tentacles” inwards to reach, monitor, and record the communications of domestic civil rights organizations. Athan Theoharis, *Spying on Americans: Political Surveillance From Hoover To The Huston Plan* 120 (1978).

The NSA’s “Operation Shamrock” demonstrates the corrosive consequences of excessive secrecy for Americans’ constitutional liberties. Operation Shamrock was “the largest governmental interception program affecting Americans” during the Cold War. Church Committee Book III, *supra*, at 740. Under Operation Shamrock, the NSA “received copies of millions of international telegrams sent to, from, or transiting the United

States.” *Id.* The NSA disseminated Shamrock’s yield among government agencies, including the FBI, CIA, Secret Service, Defense Department, and narcotics bureaus. Church Committee Book III, *supra*, at 735.

Shamrock operated in secret. In 1945, military intelligence services approached three U.S. telegraph companies, RCA Global, ITT World Communications, and Western Union International, to request their collaboration in Operation Shamrock. James Bamford, *The Puzzle Palace* 303 (1983). The companies were hesitant to cooperate, fearing that Shamrock violated section 605 of the Federal Communications Act of 1934 and that their involvement could lead to criminal prosecution for illegal electronic surveillance. *Id.* at 304. To forestall such a possibility, company executives conditioned participation upon either legal immunity from criminal prosecution or clear congressional authorization of the NSA program. Theoharis, *supra*, at 120.

The executive chose secrecy over accountability. Attorney General Clark personally assured the telegraph companies that the executive would not prosecute the companies for cooperating with Operation Shamrock. Bamford, *supra*, at 303. The executive periodically re-extended this informal agreement to the telegraph companies, making it clear that no

executive branch official – from the President down – would prosecute or expose their activities. *Id.*

The executive did not ask Congress to provide legislation explicitly authorizing the activities of Operation Shamrock. Nor did the executive approach Congress with the details of the program. Theoharis, *supra*, at 120. Congress was kept in the dark about the very existence of Shamrock’s existence until 1975, when journalists exposed the surveillance program. Bamford, *supra*, at 303. Before Congress could legislate on or even debate the legality of Operation Shamrock, the NSA killed the program. Theoharis, *supra*, at 120.

Shielded from law and public debate, Operation Shamrock grew within the hermetically sealed world of the NSA. It expanded rapidly from a surveillance program siphoning out only “enciphered telegrams of certain foreign targets” to one intercepting *every* international cable. Church Committee Book III, *supra*, at 740. *See also* Theoharis, *supra*, at 121 (“Responding to pressure from the Johnson White House and from the intelligence community . . . the NSA began intercepting messages of targeted civil rights and antiwar activists”). The daily rush of information swept up by the NSA was compared to a “firehose.” Johnson, *America’s Secret Power*, *supra*, at 64, *cf.* Lowell Bergman et al., *Spy Agency Data*

After Sept. 11 Led F.B.I. to Dead Ends, N.Y. Times, at A1 (Jan. 17, 2006) (reporting that after September 11, NSA sent “a flood” of telephone numbers, e-mail addresses and names to the FBI in search of terrorists, “requiring hundreds of agents to check out thousands of tips a month,” virtually all of which “led to dead ends or innocent Americans”).

From 1945 to 1975, the executive branch kept both Operation Shamrock and telecommunications companies’ cooperation secret from the courts and from Congress. Secrecy hid NSA activity from judicial oversight and quarantined the NSA’s corporate collaborators from possible legal sanction. Secrecy also allowed the executive to subvert Congress’s efforts to prohibit illegal electronic surveillance and the ability of federal courts to enforce any such prohibitions.

The only antidote, the Church Committee argued based on the program’s history, was openness and transparency: “Secrecy should no longer be allowed to shield the existence of constitutional, legal and moral problems from the scrutiny of all three branches of government or from the American people themselves.” Church Committee, Book II, *supra*, at 292.

B. The Church Committee's Public Disclosure Of Allegedly Sensitive Information Concerning Telegraph Companies' Involvement In Operation Shamrock Led To Greater Oversight Of NSA Surveillance Without Harming National Security.

The Church Committee's effort to bring accountability to NSA surveillance met resistance as the executive sought to suppress public disclosure about Operation Shamrock, especially information about the identity and activities of the telecommunications corporations. Then, as now, the executive raised the flag of national security to justify sweeping secrecy. But the Church Committee published the material against the executive's wishes – and no harm to national security ensued. That historical lesson speaks volumes about the dangers of the government's use of the state secrets doctrine to bar judicial review of the NSA's warrantless domestic surveillance program today.

Attorney General Edward H. Levi offered two arguments against the Church Committee's decision to publicize Operation Shamrock. First, "Levi emphasized that [public disclosure] might . . . damag[e] their business reputations. The companies might then terminate their cooperation, cutting off the NSA from a valuable intelligence source." Loch K. Johnson, *A Season of Inquiry: The Senate Intelligence Investigation* 94 (1985). Second,

he argued, public disclosure would threaten national security by exposing sensitive information to the public about federal surveillance systems. *Id.*

The Church Committee rejected these arguments. “[The Church] committee has an educational responsibility,” Senator Charles Mathias (R-Md.), one of the Church Committee’s members, argued. “[W]e should require those companies to stop and think about whether or not they are doing something illegal.” *Id.* Senator Frank Church (D-Id.) concurred, observing that “corporations indeed should be hesitant to comply with government requests – at least long enough to assure themselves that such requests were lawful and ethical.” *Id.* Public disclosure of the names of the three corporations, the Church Committee maintained, was necessary to deter future collaboration of telecommunications corporations with unauthorized NSA surveillance activities.

The executive’s fears proved unfounded: National security was not compromised by this disclosure, and “[r]elations between intelligence and the private sector endured.” L. Britt Snider, *Unlucky Shamrock: Recollections From the Church Committee’s Investigation of the NSA, Studies in Intelligence* (Winter 1999-2000), *available at*

<https://www.cia.gov/csi/studies/winter99-00/art4.html>.² In fact, pressure created by public knowledge of executive surveillance led the NSA to pay proper deference to previously neglected legal regulations. *Id.* (“Questions of legality were no longer ignored or unresolved. Agreements were put in writing and signed by the responsible officials”). Indeed, the accountability that came from disclosure prompted the “NSA to institute a system which keeps it within the bounds of US law and focused on its essential mission.” *Id.*; cf. James G. Hudec, *Unlucky Shamrock – The View From the Other Side*, *Studies in Intelligence*, (Winter/Spring 2001), available at https://www.cia.gov/csi/studies/winter_spring01/article12.pdf (oversight and openness led NSA officials to place “protection of the rights and privacy of the person” at center of internal regulations).³

In sum, the history and aftermath of the Church Committee’s exposure of NSA surveillance demonstrates that the American public *can* know the details of warrantless electronic surveillance at home without harming national security interests. And it also shows that the disinfecting sunlight of public scrutiny is necessary to ensure accountability and to

² L. Britt Snider was a lawyer on the staff of the Church Committee investigation before joining the CIA as Inspector General, a position he held when he published his recollections of the Church Committee.

³ James G. Hudec was a lawyer at the NSA Office of General Counsel during the Church Committee investigation.

prevent domestic surveillance programs from exceeding constitutional and legal bounds.

III. FISA CODIFIED THE CHURCH COMMITTEE'S RECOMMENDATIONS TO REQUIRE THAT FEDERAL COURTS REVIEW THE LEGALITY OF SURVEILLANCE PROGRAMS, EXECUTIVE CLAIMS OF STATE SECRETS PRIVILEGE NOTWITHSTANDING.

Unthinking application of the state secrets privilege in this case would abrogate the statutory scheme imposed by Congress in the form of FISA. Congress created FISA in response to the Church Committee's "revelations that warrantless electronic surveillance in the name of national security ha[d]

1. 138 CONG. REC. 21,004 (1970).

executive surveillance programs. Furthermore, FISA forbids judicial abstention from oversight in the face of executive claims of secrecy. Congress, in short, deemed the federal judiciary's full oversight powers as necessary to prevent a repetition of Cold War surveillance history. That Congressional determination should not be short-circuited by over-hasty application of the state secrets privilege.

A. FISA Requires That The Federal Judiciary Authorize and Review All Executive Electronic Surveillance, Both *Ex Ante* and *Ex Post*.

FISA makes the federal judiciary the exclusive gatekeeper of surveillance power in the United States. Per the explicit statutory command of FISA, the executive is answerable to the judiciary for its surveillance decisions – both *ex ante* and *ex post*.

FISA establishes a single statutory framework to control governmental electronic surveillance. Specifically, FISA requires that the government obtain a judicial warrant to authorize the electronic surveillance of a foreign power or agent of a foreign power. 50 U.S.C. § 1805(a)(3); *accord* S. Rep. No. 95-604 (I), at 6, 1978 U.S.C.C.A.N. at 3908. As part of FISA, Congress commanded that, along with Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (“Title III”), FISA provides “the *exclusive means* by which electronic surveillance . . . and the interception of

domestic wire, oral, and electronic communications may be conducted.” 18 U.S.C. § 2511(2)(f) (emphasis added). By requiring intelligence agencies to receive judicial authorization for its surveillance decisions in the form of a warrant, FISA “curb[s] the practice by which the Executive Branch may conduct warrantless surveillance on its own unilateral determination that national security justifies it.” S. Rep. No. 95-604 (I), at 8-9, 1978 U.S.C.C.A.N. at 3910.

Additionally, FISA grants the federal judiciary authority to police *ex post* executive compliance with FISA’s “exclusive means” provision in two ways. First, both FISA and Title III impose severe civil and criminal sanctions upon those who conduct surveillance without statutory authority. 50 U.S.C. §§ 1809, 1810; *see also* 18 U.S.C. §§ 2511, 2520. Second, along with Title III, FISA creates a private cause of action enabling any subject of illegal electronic surveillance to bring a lawsuit in federal court against both governmental and involved private parties. *See* 18 U.S.C. § 2520(a) (creating civil cause of action for interception of communications in violation of Title III); 50 U.S.C. § 1810 (same for electronic surveillance in violation of FISA); *see also* 18 U.S.C. § 2707(a) (same for unlawful disclosure by communications providers); 50 U.S.C. § 1809 (prohibiting “electronic surveillance under color of law except as authorized by statute”):

47 U.S.C. § 605(e)(3)(A) (same for unlawful disclosures by communications providers under the Federal Communications Act of 1934).

The Church Committee described the abuses of executive surveillance as the result of the “clear and sustained failure . . . to control the intelligence community and to ensure its accountability.” Church Committee Book II, *supra*, at 15 Congress sought to avoid the mistakes of the past through comprehensive federal judicial oversight by enacting FISA.

B. FISA Requires That Federal Courts Exercise Oversight of Executive Surveillance, Regardless of Executive Invocations of State Secrecy Privileges.

Excessive secrecy precludes meaningful oversight. The Church Committee revealed that secrecy shielded executive malfeasance during the Cold War. Congress drafted FISA with this history lesson in mind, ensuring not only that federal courts would have statutory authority to review the legality of executive surveillance but also that executive claims of secrecy would not render this judicial authority a nullity.

FISA addresses the question of classified evidence, and provides the federal court with tailored instructions about how to deal with the problem:

[W]henever any motion or request is made by an aggrieved person . . . to discover or obtain applications or orders or other materials relating to electronic surveillance . . . 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 a disclosure is necessary to make an *accurate determination of the legality of the surveillance*.

50 U.S.C. § 1806(f) (emphases added). This provision incorporated a response to the Church Committee's finding that excessive judicial deference allowed for governmental abuse of surveillance powers. It *requires* courts to exercise oversight of electronic surveillance and, when *the court* deems necessary, to disclose sensitive materials to the aggrieved party. That requirement stands even when the executive believes that such oversight might endanger "national security."

The government, by invoking the state secrets doctrine in this case, seeks precisely the kind of unquestioned deference that Congress considered and rejected in FISA. By providing a clear statutory regime for handling of secrecy claims, FISA displaces plenary operation of the common law state secrets privilege and helps ensure federal courts can effectively play their appointed role in the Constitution's system of checks and balances. *See Hepting v. AT&T*, 439 F. Supp. 2d 974, 980 (N.D. Cal. 2006) ("The state secrets privilege is a common law evidentiary rule") (citing *In re United States*, 872 F.2d 472, 474-475 (D.C. Cir. 1989)); *see also Fairfax's Devisee*

v. Hunter's Lessee, 11 U.S. (7 Cranch) 603, 623 (1812) (“The common law.... ought not to be deemed repealed, *unless the language of a statute be clear and explicit for this purpose*”) (emphasis added).

If the executive branch believes the balance between secrecy and oversight struck by FISA to be inadequate, it can always ask Congress to amend the act. FISA has been amended numerous times since it was enacted in 1978, including numerous times after September 2001. *See, e.g.*, USA PATRIOT Act, Pub. L. No. 107-56, § 218, 115 Stat. 272, 291 (2001) (amending 50 U.S.C. § 1804(a)(7)(B)) (amending FISA’s warrant requirement so that only “a significant purpose,” rather than “a primary purpose,” of electronic surveillance must be to obtain foreign intelligence information). Instead, the Executive has sought to circumvent FISA by asking this Court to “take measures incompatible with the expressed . . . will of Congress,” undermining “the equilibrium established by our constitutional system.” *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 609, 637-38 (1952) (Jackson, J., concurring); *accord Hamdan v. Rumsfeld*, 126 S. Ct. 2749, 2774 n.23 (2006).

Congress designed and enacted FISA to recalibrate the balance between oversight and secrecy, and prevent a repeat of harms that accrued from decades of secret warrantless surveillance to groups like *amici* and

other Americans. AT&T's involvement in the new program of NSA surveillance is a proper subject of judicial oversight. The Judiciary's failure to exercise that oversight would violate Congress' express intent in enacting FISA and effectively ignore the lessons of history by repeating the mistakes of America's Cold War past.

CONCLUSION

The history of Cold War domestic intelligence abuses, the Church Committee's inquiry into these abuses, and Congress's enactment of FISA all illustrate the axiom that should guide this Court: Meaningful judicial oversight of warrantless domestic surveillance should trump secrecy. Absent such oversight, intelligence powers inevitably turn from foreign foes toward domestic political opponents, from real enemies of the nation toward those whose views the executive branch disdains. And they do so under an ambiguous label of "national security" that has historically been abused.

Accordingly, for the aforementioned reasons, *amici* urge this Court to affirm the decision of the district court.

Dated: May 2, 2007

Respectfully submitted,

Jonathan Hafetz
Aziz Z. Huq
Frederick A.O. Schwarz, Jr.
BRENNAN CENTER FOR JUSTICE
AT NYU SCHOOL OF LAW
161 Avenue of the Americas, 12th Fl.
New York, New York 10013
(212) 998-6730

Marc Van Der Hout
Beth Feinberg
VAN DER HOUT, BRIGAGLIANO
& NIGHTINGALE, LLP
180 Sutter St., Fifth Floor
San Francisco, CA 94104
Telephone: (415) 981-3000
Facsimile: (415) 981-3003

Counsel for *Amici Curiae*

By: 
Marc Van Der Hout

**CERTIFICATE OF COMPLIANCE TO
FED. R. App. P. 32 (a)(7)(C) AND NINTH CIRCUIT
RULE 32-1 FOR CASE NUMBER 06-15085**

I certify that:

1. Pursuant to Fed. R. App. P. 32(a)(7)(C) and Ninth Circuit Rule 32-1, the attached opening/answering/reply/cross-appeal brief is
 - Proportionately spaced, has a typeface of 14 points or more and contains _____ words, (opening, answering, and the second and third party briefs filed in cross-appeals must not exceed 14,000 words; reply briefs must not exceed 7,000 words),
OR IS
 - Monospaced, has 10.5 or less characters per inch and contains words or _____ lines of text (opening, answering, and the second and third briefs filed in cross-appeals must not exceed 14,000 words or 1,300 lines of text; reply briefs must not exceed 7,000 words or 650 lines of text)

2. The attached opening/answering/reply/cross-appeal brief is **not** subject to the type-volume limitations of Fed. R. App. P. 32(a)(7)(B) because
 - This brief complies with Fed. R. App. 32(a)(1)-(7) and is a principal brief of no more than 30 pages or a reply brief of no more than 15 pages;
 - This brief complies with a page or size-volume limitation established by separate court order dated _____ and is
 - Proportionately spaced, has a typeface of 14 points or more and contains _____ pages or _____ words,
OR IS
 - Monospaced, has 10.5 or fewer characters per inch and contains _____ pages or _____ words or _____ lines of text.

3. Pursuant to Fed. R. App. 29(d) and Ninth Circuit Rule 32-1, the attached AMICUS BRIEF is proportionally spaced, has a type face of 14 points or more and contains 7,000 words or less,

- OR IS
- Monospaced, has 10.5 or fewer characters per inch and contains not more than 7,000 words or 650 lines of text,
- OR IS
- Not subject to the type-volume limitations because it is an amicus brief of no more than 15 pages and complies with Fed. R. App. P. 32(a)(1)(5).

Date: May 2, 2007



Marc Van Der Hout

Counsel for *Amici Curiae*

PROOF OF SERVICE BY FIRST CLASS MAIL

I, Beth Feinberg, the undersigned, say:

I am over the age of eighteen years and not a party to the within action or proceedings; my business address is: Van Der Hout, Brigagliano & Nightingale, LLP, 180 Sutter St, Fifth Floor, San Francisco, California 94104.

On May 2, 2007, I caused to be served the within:

**BRIEF OF *AMICI CURIAE* NATIONAL ASSOCIATION FOR THE
ADVANCEMENT OF COLORED PEOPLE, AMERICAN-ARAB ANTI-
DISCRIMINATION COMMITTEE, ASIAN AMERICAN LEGAL
DEFENSE AND EDUCATION FUND, JAPANESE AMERICAN
CITIZENS LEAGUE, THE LEAGUE OF UNITED LATIN AMERICAN
CITIZENS, AND UNITED FOR PEACE AND JUSTICE
SUPPORTING PLAINTIFFS – APPELLEES URGING AFFIRMANCE**

on the opposing counsel and Department of Homeland Security by depositing two true copies, thereof, enclosed in a sealed envelope with postage fully pre-paid, in a mailbox regularly maintained by the Government of the United States at San Francisco, California, to each person listed below addressed as follows:

Peter D. Keisler
Carl J. Nichols
Anthony J. Coppolino
Andrew H. Tannenbaum
Joseph Hunt
U.S. Department of Justice
Civil Div., Federal Programs Branch
20 Massachusetts Ave. N.W., Rm. 6102
Washington, D.C. 20001

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

Douglas N. Letter
Thomas M. Bondy
Anthony A. Yang
U.S. Department of Justice
Civil Division, Appellate Staff
950 Pennsylvania Ave. N.W., Rm. 7513
Washington, D.C. 20530-0001

Paul D. Clement
Gregory G. Garre
Daryl Joseffer
Office of the Solicitor General
950 Pennsylvania Ave. NW, Suite 5143
Washington, D.C. 20530-2201

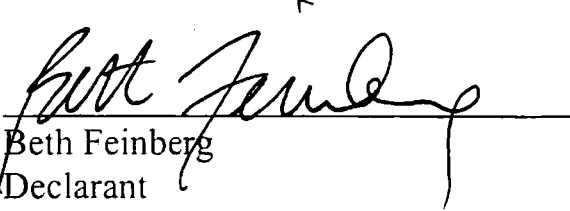
Bruce A. Ericson
Kevin M. Fong
Marc H. Axelbaum
Jacob R. Sorensen
Pillsbury Winthrop Shaw Pittman LLP
50 Fremont Street
San Francisco, CA 94105

Cindy Cohn
Lee Tien
Kurt Opsahl
Kevin S. Bankston
James S. Tyre
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110

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

Marcia Hofmann, Staff Attorney
Electronic Frontier Foundation
1875 Connecticut Ave. NW, Suite 650
Washington, DC 20009

Executed on May 2, 2007 at San Francisco, California. I declare under penalty of perjury that the foregoing is true and correct.


Beth Feinberg
Declarant