THE WALLS (AND WIRES) HAVE EARS: THE BACKGROUND AND FIRST TEN YEARS OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978

AMERICO R. CINQUEGRANA†

On the afternoon of January 14, 1980, agents of the Federal Bureau of Investigation recorded the following conversation between Vladimir Sorokin, an official from the Soviet Embassy in Washington, D.C., and an unidentified caller.*

> . . . . Vladimir Sorokin speaking.
>
> . . . .
>
> Caller: Ah, I have something I would like to discuss with you I think that would be very interesting to you.
>
> . . . .
>
> Is there any way to do so in, in, in, ah, confidence or in privacy?
>
> Sorokin: Maybe you can, ah, name yourself?
>
> Caller: Ah. . .ah, on the telephone it would not be wise.
>
> Sorokin: I see.
>
> . . . .
>
> I come from, I, I, I am in, with the United States government.

The caller was determined later to have been Ronald W. Pelton, a former employee of the National Security Agency, and the subject was serious: espionage against the United States. This and other conversations that constituted critical evidence in the espionage prosecution of Pelton** were acquired through electronic surveillance by the FBI under the authority of the Foreign Intelligence Surveillance Act of 1978. In light of the Act's tenth anniversary, this commentary discusses the legal and political foundations for that statute, its contents, and the consequences of its implementation. The commentary concludes by discussing the results of the Act's subjugation to judicial scrutiny since its

---

† Deputy Counsel for Intelligence Policy, Office of Intelligence Policy and Review, United States Department of Justice. B.A. 1968, University of New Hampshire, J.D. 1973 University of Virginia. The views expressed in this article are those of the author and do not necessarily represent those of the Justice Department.

* Full transcript on file at the University of Pennsylvania Law Review.

** United States v. Pelton, 835 F.2d 1067 (4th Cir. 1987), *cert. denied,* 108 S.Ct 1741 (1988).

enactment, and several potential amendments that merit further consideration by Congress.

I. INTRODUCTION

The Foreign Intelligence Surveillance Act of 1978 ("FISA," "the Act")[1] embodies legal principles developed over decades by the Supreme Court, Congress and the Executive, in their efforts to relate the terms of the fourth amendment to electronic surveillance.[2] The Act was a product of years of debate concerning whether the President possessed inherent constitutional authority to approve warrantless electronic surveillance for national security purposes.[3]

The terms of the Act, its legal foundation, and its legislative history illustrate the competing interests and political principles that operate in a constitutional democracy in which power is shared among three independent branches of government. Perhaps the most significant product of the turmoil that engulfed the national security bureaucracies in the 1970s, the Act attempts to apply domestic law enforcement principles to activities conducted for national security purposes.

In crafting FISA, both Congress and the executive branch were forced to compromise substantially in order to agree on an effective regulatory scheme. In this respect, FISA is a prime example of the different perspectives and purposes that shape discussion of congressional

---

[1] Pub. L. No. 95-511, 92 Stat. 1783 (codified at 50 U.S.C. §§ 1801-11 (1982 & Supp. III 1985), 18 U.S.C. §§ 2511, 2518-19 (1982 & Supp. IV 1986)).

[2] The fourth amendment provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. CONST. amend. IV.

[3] *See* SENATE COMM. ON THE JUDICIARY, REPORT TO ACCOMPANY S. 1566, S. REP. NO. 604, 95th Cong., 1st Sess. 7-9 (1977); *Foreign Intelligence Surveillance Act of 1977: Hearings on S. 1566 Before the Subcomm. on Criminal Laws and Procedures of the Senate Comm. on the Judiciary,* 95th Cong., 1st Sess. 1-3 (1977) (statement of Senator Kennedy); *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 Senate Comm. on the Judiciary,* 94th Cong., 2d Sess. 1-4 (1976) (statements of Senators McClellan and Kennedy); *Electronic Surveillance Within the United States for Foreign Intelligence Purposes: Hearings on S. 3197 Before the Senate Subcomm. on Criminal Laws and Procedures of the Senate Comm. on the Judiciary,* 94th Cong., 2d Sess. 1-4 (1976); *Electronic Surveillance Within the United States for Foreign Intelligence Purposes: Hearings on S. 3197 Before the Subcomm. on Intelligence and the Rights of Americans of the Senate Select Comm. on Intelligence,* 94th Cong., 2d Sess. 4-5 (1976) [hereinafter *Electronic Surveillance Hearings*] (statement of Senator Kennedy).

regulation of executive branch activities in general, and intelligence activities in particular. The genesis of FISA also highlights the uncertainty caused by reliance on the judicial process to establish rules of behavior for the executive branch, the influences shaping congressional action, and the Executive's proclivity for occupying the power vacuums that result from the ponderous nature of the legislative and judicial processes.

Thus, review of the foundation, creation, and application of the Foreign Intelligence Surveillance Act presents a basis for understanding interbranch conflict and collaboration. This commentary will trace the development of FISA through the painfully slow elaboration of legal and political limits on controversial intelligence activities. Particular focus will be placed upon how the Executive makes use of the discretion that is paced in its hands by default as a result of intermittent and often confused judicial decisions and the lack of a congressional consensus. Finally, as mentioned, a number of potential statutory improvements are discussed.

II. HISTORICAL FOUNDATIONS

A. *Early Treatment of Electronic Surveillance*

National security interests and electronic surveillance converged in 1918 when a criminal penalty was enacted to protect from espionage the telephone system operated by the United States government during World War I.[4] Before 1918, and after the criminal penalty expired in 1919, warrantless wiretapping by the executive branch was a common practice.[5] It was not until 1928 that the issue came before the Supreme Court, in *Olmstead v. United States*.[6]

Olmstead resulted in a sharp 5-4 division, with the Court favoring the admissibility in a criminal trial of private telephone conversations intercepted through wiretaps. Chief Justice Taft, speaking for the majority, emphasized the fact that "voluntary conversations secretly overheard" could not be equated with material "things" seized by the government.[7] Since the persons using the telephone intended to project their words outside their homes, and there had been no physical intru-

---

[4] Act of October 29, 1918, Pub. L. No. 65-230, ch. 197, 40 Stat. 1017, 1017-18.

[5] *See* Donnelly, *Comments and Caveats on the Wire Tapping Controversy*, 63 YALE L.J. 799, 799-800 (1954). In 1924 and 1928, Attorneys General Stone and Sargent prohibited the Justice Department's Federal Bureau of Investigation from using this technique on ethical grounds. *See id.*; *Electronic Surveillance Hearings*, *supra* note 3, at 23 (reprinted testimony of Attorney General Levi).

[6] 277 U.S. 438 (1928).

[7] *Id.* at 464.

sion, the Court held that this mode of acquisition was not regulated by the fourth amendment.[8]

The majority, rejecting an "enlarged and unusual meaning" of the fourth amendment,[9] concluded that Congress should enact protective legislation if it believed that the use of intercepted communications as evidence in federal criminal trials should be limited.[10] In dissent, Justice Brandeis argued that the Court's interpretation of the fourth amendment should guard against the increasingly sophisticated means available to the government to invade privacy and use in court "what is whispered in the closet."[11]

In resolving the constitutional issue in favor of a property-oriented view of fourth amendment rights, rather than one based on a notion of individual privacy, the *Olmstead* decision removed electronic surveillance techniques not involving physical intrusions from fourth amendment scrutiny for almost ten years. This left control of such activities squarely within the discretion of the executive branch.

B. *Thermidor and the Deluge*

Olmstead set the stage for an enduring conflict between the executive and legislative branches by allowing executive branch surveillance involving no actual physical intrusion, yet stirring congressional interest in regulating the technique and broadening individual protections. The conflict, which began in the domestic law enforcement context, eventually spilled over into the national security setting where new considerations complicated and exacerbated the debate.

In 1931, in the face of several unsuccessful congressional proposals and an executive study of the matter,[12] Attorney General William D. Mitchell concluded that electronic surveillance, while perhaps raising ethical issues, was not unlawful. He authorized high-level officials in charge of "exceptional cases" involving "substantial and serious"

---

[8] *Id.* at 464-66.

[9] *Id.* at 465-66.

[10] *Id.* at 466.

[11] *Id.* at 474.

> The progress of science in furnishing the Government with means of espionage is not likely to stop with wire-tapping. Ways may some day be developed by which the Government . . . will be enabled to expose to a jury the most intimate occurrences of the home. . . . Can it be that the Constitution affords no protection against such invasions of individual security?

Id.

[12] *See* S. 3344, 71st Cong., 3d Sess. (1931); *Hearings Before the House Comm. on Expenditures in the Exec. Depts.: Wire Tapping and Law Enforcement*, 71st Cong., 3rd Sess., 76 (Testimony of William D. Mitchell) (1931).

crimes to approve wiretapping.[13] Meanwhile, growing congressional interest in regulating electronic surveillance led to a 1933 appropriations bill rider forbidding the use of any authorized funds for wiretapping to enforce prohibition laws.[14] The Federal Communications Act of 1934 went even farther and barred interception and disclosure of any wire or radio communication.[15] Interpreting the 1934 Communications Act in 1937, the Supreme Court held in *Nardone v. United States*[16] that an electronic interception of a telephone conversation, and disclosure of the evidence so obtained, was unlawful.[17] For the next eleven years, this decision precluded the introduction of evidence obtained by electronic surveillance. The technique continued to be used, however, because the Executive construed *Nardone* as preventing use of electronic surveillance only when it was combined with disclosure of its fruits outside of the government. In the absence of clear and compelling judicial restraint, the executive branch left to Congress the debate concerning whether and what types of limits should be imposed.[18]

As the world political situation darkened with the onset of World War II, the national security aspects of electronic surveillance rose in importance. In May 1940, the House of Representatives considered and approved a Joint Resolution affirming the Federal Bureau of Investigation's authority to conduct wiretapping for national security purposes.

---

[13] *See Electronic Surveillance Hearings*, *supra* note 3, at 24 (statement by Attorney General Levi). This early guidance resulted in the later practice, incorporated into statute, that federal wiretapping for law enforcement purposes be limited to the most serious crimes such as kidnapping, apprehension of desperate criminals, sabotage, and espionage.

[14] Act of Mar. 1, 1933, Pub. L. No. 387, ch. 144, 47 Stat. 1371, 1381 (1933). Several proposals to limit federal wiretapping or use of its fruits had been unsuccessful during the previous year. *See* H.R. 23, 72d Cong., 1st Sess. (1931); S. 1396, 73d Cong., 1st Sess.(1931); 74 CONG. REC. 3928 (1931); 75 CONG. REC. 4541 (1932).

[15] Federal Communications Act of 1934, Pub. L. No. 73-416, ch. 652, 48 Stat. 1064, 1103-04 (1934) (codified as amended at 47 U.S.C. § 605 (Supp. III 1985)) [hereinafter 1934 Communications Act]. The predecessor section can be found in the Radio Act of 1927, Pub. L. No. 632, ch. 169, 44 Stat. 1162, 1172 (1927).

[16] 302 U.S. 379 (1937).

[17] *Id.* at 382. The Court later extended this holding to bar the use of additional evidence derived from the intercepted communications. Nardone v. United States, 308 U.S. 338, 340 (1939). *But see Justice Department Bans Wiretapping; Jackson Acts on Hoover Recommendation*, N.Y. Times, Mar. 18, 1940, § 1, at 1, col. 3 (noting that it was public knowledge in 1940 that the FBI had engaged in "wire tapping since 1931, although the practice [had] been held illegal by the Supreme Court").

[18] "Whether a criminal or suspected criminal should be completely protected in his right of privacy, or whether, in the interests of society, an invasion of such right of privacy should be permitted . . . involves a question of balance, which is peculiarly within the province of the legislative branch . . . ." S. REP. No. 1790, 75th Cong., 3d Sess. 4 (1938) (letter of Attorney General Cummings to Sen. Wheeler, dated April 26, 1938).

The Senate, however, failed to approve the resolution.[19] President Roosevelt then decided to act unilaterally and expressed his desire to Attorney General Jackson that "listening devices" be used when "grave matters involving defense of the nation," such as espionage or subversion, might be involved. Such surveillance was to be limited to aliens insofar as possible.[20]

The momentum which the executive branch's surveillance activities had gathered during World War II was not diminished by the cessation of hostilities in 1945. In July 1946, President Truman approved broader use of electronic surveillance in cases "vitally affecting the domestic security". [21] Eight years later, Attorney General Brownell empowered FBI Director J. Edgar Hoover to conduct trespassory electronic surveillance without prior Attorney General approval when the FBI determined that such intelligence collection was in the national interest.[22]

Meanwhile, during the years following *Olmstead*, the courts were moving from a fourth amendment jurisprudence based upon protection of individual property to one based upon the protection of individual privacy interests. In a 1942 decision, the Supreme Court refused to overrule *Olmstead* and determined that placing a "detectaphone" against a wall to overhear conversations in an adjoining office was lawful because it involved no physical trespass. The forceful tone of Justice Murphy's dissent,[23] however, and the fact that Justices Stone and Frankfurter also wished to overrule *Olmstead*,[24] indicated that by a

---

[19] H.R.J. Res. 553, 76th Cong., 3d Sess. (1940); N. Y. Times, *supra* note 17, § 1, at 1, col. 3. *See also Hearings on Wiretapping, Eavesdropping, and the Bill of Rights, before the Subcomm. on Constitutional Rights of the Senate Judiciary Comm. pursuant to S. 284*, 85th Cong., 2d Sess. 199 (1958).

[20] *See Electronic Surveillance Hearings*, *supra* note 3, at 24 (statement by Attorney General Levi).

[21] The President apparently considered rescinding the order when it was determined later to be more expansive than the Roosevelt order. *See* S. REP. NO. 604, *supra* note 3, at 10 n.10.

[22] *See Electronic Surveillance Hearings*, *supra* note 3, at 25 (statement by Attorney General Levi); HOUSE PERMANENT SELECT COMM. ON INTELLIGENCE, REPORT TO ACCOMPANY H.R. 7308, H.R. REP. NO. 1283, 95th Cong., 2d Sess., pt. 1, at 16 (1978).

[23] Goldman v. United States, 316 U.S. 129 (1942). As Justice Murphy observed:

> The search of one's home or office no longer requires physical entry, for science has brought forth far more effective devices for the invasion of a person's privacy. . . . Whether the search of private quarters is accomplished by placing on the outer walls of the sanctum a detectaphone that transmits to the outside listener the intimate details of a private conversation, or by new methods of photography that penetrate walls or overcome distances, the privacy of the citizen is equally invaded . . .

Id. at 139 (footnotes omitted).

[24] *Id.* at 136.

slight shift in the Court's thinking, such conversations could be treated as "effects" and brought within the protection of the fourth amendment.

Olmstead was further weakened in 1961 by the Court's holding that the interception of oral communications could violate the fourth amendment, because a trespass had technically occurred when police officers used a "spike" microphone that was driven from an adjacent row house through the wall of a defendant's house and into contact with a heating duct which served to transmit conversations occurring throughout the house.[25] The Court refused to abandon the requirement that there be a physical trespass in order to merit fourth amendment protection, but did not enter into a detailed analysis of property rights, and indicated a growing recognition of the corrosive effects of new surveillance techniques on privacy interests.[26]

Nonetheless, while the courts and Congress continued to contemplate the matter, almost 7000 wiretaps and 2200 microphone surveillances were used by the Executive between 1940 and the mid-1960s in internal security investigations concerning foreign intelligence agents and Communist Party leaders, as well as major criminal activities.[27] In June 1965, President Lyndon Johnson limited the use of wiretaps to investigations involving the collection of intelligence affecting the national security and required Attorney General approval for both wiretaps and microphone surveillance.[28] Even under these restrictions, however, approximately 1,350 warrantless wiretaps and 250 microphone installations were authorized from 1965 through 1974.[29]

---

[25] Silverman v. United States, 365 U.S. 505, 506-509 (1961).

[26] The Court described, but did not find it necessary to deal with, the "frightening paraphernalia which the vaunted marvels of an electronic age may visit upon human society":

> We are favored with a description of "a device known as the parabolic microphone which can pick up a conversation three hundred yards away." We are told of a "still experimental technique whereby a room is flooded with a certain type of sonic wave," which, when perfected, "will make it possible to overhear everything said in a room without ever entering it or even going near it." We are informed of an instrument "which can pick up a conversation through an open office window on the opposite side of a busy street."

Id. at 508-09.

[27] *See Electronic Surveillance Hearings*, *supra* note 3, at 25 (statement by Attorney General Levi).

[28] *See id.* at 26.

[29] *Id.* at 26.

C. *Property Rights Succumb to Privacy Interests*

The activities of the executive branch, abetted by the inadequacy of congressional supervision of information gathering techniques, provided the Supreme Court with an impetus to review once again the fourth amendment limits on electronic surveillance in *Katz v. United States*.[30] *Katz* afforded the Court an opportunity to recognize the threats to privacy interests posed by modern technology — in this case, an FBI microphone surveillance of a public telephone booth — and to abandon at last its reliance on the existence of a physical trespass before invoking the protection of the fourth amendment. The Court, in a now-famous phrase, ruled that "the Fourth Amendment protects people, not places"[31] and formulated a new test for the validity of any search, seizure, or surveillance in terms of privacy expectations rather than property interests.[32] Fourth amendment protection now focused on individuals, not locations, and extended to surveillance techniques not requiring a physical intrusion.

The Court's gratuitous discussion in *Katz* regarding surveillance activities undertaken in furtherance of national security interests was critical to the development of FISA. In a footnote that proved to have lasting historical significance, the Court expressly preserved national security surveillance from the reach of its decision that a warrant would be required for electronic surveillance.[33] Justice White emphasized this point in a concurring opinion dwelling on the unique requirements of electronic surveillance for national security purposes. He noted the authorization of such activities by a succession of Presidents, concluding that no prior judicial review should be required if the President or the Attorney General found surveillance reasonable under the circumstances.[34]

This distinction between law enforcement and national security requirements for electronic surveillance was subsequently recognized by Congress as well. In 1968, Congress accepted the judicial and executive invitation, outstanding since *Olmstead,* to define more clearly the proper use of electronic surveillance techniques in criminal investigations. In enacting Title III of the Omnibus Crime Control and Safe

---

[30] 389 U.S. 347, 353 (1967) (overruling *Olmstead* and *Goldman*).

[31] *Id.* at 351.

[32] "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." *Id.* at 351-52 (citations omitted).

[33] *Id.* at 358 n.23.

[34] *Id.* at 363-64.

Streets Act,[35] Congress drew upon principles discussed in the *Katz* decision. The 1968 Omnibus Act established a detailed procedure for the issuance of a warrant prior to using microphone surveillance or wiretapping for law enforcement purposes, based on a finding by a neutral magistrate of probable cause to believe that a serious crime had been or was about to be committed.[36]

The statute specifically disclaimed any intention that its provisions, or those of the 1934 Communications Act, should be read to affect the constitutional powers of the President to protect the United States against hostile foreign powers, to obtain foreign intelligence information, to protect the government against efforts to overthrow it by force, or to guard against any other "clear and present danger."[37] Further, information collected under these circumstances could be received in evidence in any proceeding, so long as the surveillance was determined to be "reasonable."[38] This provision could be, and indeed was, fairly understood by the executive branch as tacit congressional acceptance of the claimed inherent power of the President to authorize these activities under the circumstances described so vaguely in the statute.[39]

D. *The Greening of Inherent Authority*

Congress, like the Supreme Court, was not prepared in 1968 to regulate the Executive's claim of inherent power to conduct warrantless electronic surveillance for national security purposes. This deference, like prior congressional inaction, perpetuated the ability of the executive branch to occupy the field and conduct electronic surveillance without prior judicial review when deemed necessary.[40] Given the turbulent

---

[35] Pub. L. No. 90-351, 82 Stat. 212 (codified as amended at 18 U.S.C. §§ 2510-2520 (1968)) [hereinafter 1968 Omnibus Act].

[36] 18 U.S.C. § 2518(3)(a), (b) (1968).

[37] 18 U.S.C. § 2511(3) (1968).

[38] *Id.*

[39] *See, e.g.*, Zweibon v. Mitchell, 516 F.2d 594, 653 n.191 (D.C. Cir. 1975), *cert. denied*, 425 U.S. 944 (1976) (quoting a worried senator during floor debate on § 2511 (3): "As I read it — and this is my fear — we are saying that the President . . . could [unilaterally] declare . . . draft dodgers, Black Muslims, the Ku Klux Klan, or civil rights activists to be a clear and present danger to the structure or existence of the Government.").

[40] The executive branch rationale for not obtaining prior judicial approval of such activities included assertions that the judiciary was not competent to assess the validity of intelligence-related surveillance; that the courts did not operate under the security measures necessary to protect the sensitive information involved; that the absence of a criminal investigation (in a strict sense) reduced the need for such review; that the courts could not move rapidly enough to cope with urgent developments; and that judicial review would pose a debilitating burden on the Executive's vital freedom to act in these matters. *See id.* at 641.

upheavals of the 1960s, it became almost inevitable that the Court and Congress would have to clarify once more the extent to which the Executive's claims of inherent power were to be recognized.

These limits were discussed to some extent in the lower courts.[41] The seminal case in the development of the law of national security surveillance, however, proved to be the so-called "*Keith*" case, *United States v. United States District Court*, decided by the Supreme Court in 1972.[42] Among the defendants in *Keith*, who were alleged to have conspired to destroy government property, was one who had been charged with bombing a CIA office in Michigan.[43] Pretrial proceedings revealed that this defendant's conversations had been overheard by the government in the course of a warrantless electronic surveillance authorized by the Attorney General in order to acquire intelligence necessary to protect against attacks and subversion by domestic organizations.[44]

The Court concluded that the reservation of presidential authority in the 1968 Omnibus Act[45] represented merely a neutral statement by Congress that the President has some degree of power in the areas of national defense and internal security and was not an attempt to "expand," "contract," or "define" that power.[46] Thus, it was necessary to examine the constitutional, rather than the statutory, basis for the surveillance authority asserted on the President's behalf.[47]

The Court was careful to point out that the case before it concerned only surveillance of domestic organizations — those having no significant connections to foreign powers or their agents — deemed to threaten the existence of the government.[48] Moreover, the Court was quick to concede that the President has a fundamental duty to protect against unlawful subversion and that a government's basic function is to defend itself and its citizens.[49] The Court was well aware, however, that the difficulty of defining the inherently ambiguous power to protect "domestic security" is compounded in cases involving national se-

---

[41] *See, e.g.*, United States v. Hoffman, 334 F. Supp. 504, 506-08 (D.D.C. 1971) (rejecting the government's argument that foreign intelligence and domestic affairs are "inextricably intertwined," and holding four of five warrantless surveillances unlawful because they were intended to collect evidence against dissident domestic organizations, not foreign intelligence).

[42] 407 U.S. 297 (1972).

[43] *Id.* at 299.

[44] *Id.* at 300.

[45] *See supra* notes 37-39 and accompanying text.

[46] *Keith*, 407 U.S. at 303-08 ("In short, Congress simply left presidential powers where it found them.").

[47] *Id.* at 308.

[48] *Id.* at 308, 309 & n.8.

[49] *Id.* at 310.

curity surveillance because first amendment concerns of stifling debate and discussion, as well as fourth amendment values, are necessarily implicated.[50]

The Court balanced the danger to individual privacy against the potential for frustrating governmental objectives and held that the fourth amendment required prior judicial review of any electronic surveillance for domestic security purposes.[51] Although the Court rejected the government's arguments that courts lacked the necessary expertise and security to evaluate this type of intelligence activity, it emphasized that its holding did not extend to surveillance involving foreign powers or their agents.[52]

Furthermore, the Court urged Congress to enact legislation that would supplement the 1968 Omnibus Act and strike a constitutionally permissible balance between criminal and domestic security surveillance so as to create a more workable framework for judicial review.[53] Because domestic security surveillance implicates different policies and is for different purposes than those contemplated by the "ordinary crime" standards of the 1968 Omnibus Act, different application, duration, and reporting requirements might be appropriate, and a specially designed court might be useful for sensitive cases.[54]

No congressional action has ever been taken regarding the use of electronic surveillance in the domestic security area. Nonetheless, the Court's explanation in *Keith* regarding the flexibility that would be permissible under the fourth amendment paved the way for FISA and its carefully tailored provisions for surveillance of foreign powers and their agents in the United States.

E. *From* Keith *to FISA*

The Supreme Court in *Keith* had not addressed the legality of warrantless electronic surveillance undertaken by the Executive for genuine national security purposes. Lower federal courts, however, continued to grapple with this issue and their opinions also made important contributions to the shaping of FISA. Of the five federal courts of appeals that examined warrantless electronic surveillance activities,

---

[50] *Id.* at 314 ("[P]rivate dissent, no less than open public discourse, is essential to our free society").

[51] *Id.* at 313-15, 319, 321 (citing United States v. Smith, 321 F. Supp. 424, 425-26 (D.C. Cal. 1971) for the proposition that warrantless surveillance of situations involving foreign powers may be constitutional).

[52] *Id.* at 321, 322 & n.20.

[53] *Id.* at 322-24.

[54] *Id.* at 322.

four readily accepted the existence of a foreign intelligence exception to the warrant requirement based on the legal and policy arguments put forward by the Executive.

Typically, these arguments reflected a concern for the efficiency and expertise of the nation's foreign intelligence process and the deleterious effects that might result from judicial interference. For instance, the Fifth Circuit in *United States v. Brown*[55] upheld the legality of an Attorney General-authorized warrantless surveillance that was targeted at the object of a genuine foreign intelligence investigation and incidentally acquired the communications of a black activist, H. Rap. Brown.[56] Similarly, the Third Circuit held in *United States v. Butenko*[57] that warrantless surveillance whose "primary purpose" was to obtain foreign intelligence information concerning the activities of foreign powers within the United States was lawful even when conversations of American citizens were acquired.[58] The court noted that the strong public interest in the efficient operation of the nation's intelligence process could be frustrated if officials were required to interrupt their operations to "rush to the nearest available magistrate."[59]

The Ninth Circuit in *United States v. Buck*[60] also held that electronic surveillance of foreign powers and their agents was considered a "recognized exception" to the general warrant requirement of the fourth amendment.[61] The Fourth Circuit, in *United States v. Truong*,[62] wrestled with the difficult issue of when an investigation becomes a search for evidence of a crime rather than an intelligence gathering effort, but clearly recognized a warrant exception flowing from the Executive's presumed expertise in the foreign intelligence area. The court would not accept the defendant's assertions that the activity must be "solely" related to national security issues, nor the government's claim that "any" degree of foreign intelligence interest would suffice.[63] Thus, only information acquired after the date at which the court determined the investigation had become primarily criminal in nature

---

[55] 484 F.2d 418 (5th Cir. 1973), *cert. denied*, 415 U.S. 960 (1974). This circuit had held prior to *Keith* that a foreign intelligence surveillance authorized by the Attorney General did not violate the fourth amendment. United States v. Clay, 430 F.2d 165 (5th Cir. 1970), *rev'd on other grounds*, 403 U.S. 698 (1971).

[56] *Brown*, 484 F.2d at 425-26.

[57] 494 F.2d 593 (3d Cir.) (en banc), *cert. denied*, 419 U.S. 881 (1974).

[58] *Id.* at 606.

[59] *Id.* at 605.

[60] 548 F.2d 871 (9th Cir.), *cert. denied*, 434 U.S. 890 (1977).

[61] *Id.* at 875-76.

[62] 629 F.2d 908 (4th Cir. 1980).

[63] *Id.* at 912-16.

was suppressed as the fruit of unlawful warrantless surveillance.[64]

The only federal court to cast fundamental doubt upon the constitutional basis for this type of warrantless surveillance was the Court of Appeals for the District of Columbia in the 1975 decision, *Zweibon v. Mitchell*.[65] The case involved individual damages claims relating to warrantless FBI electronic surveillance of Jewish Defense League members suspected of violent activities against Soviet facilities in the United States.[66] The court recited the conclusion from *Keith* that a warrant is required for electronic surveillance of a domestic organization that is neither a foreign power nor an agent of, or collaborator with, such a power, regardless of whether the group's activities might have some impact on U.S. foreign relations.[67]

Yet a plurality of the court went further and expressed its belief that "absent exigent circumstances, *all* warrantless electronic surveillance is unreasonable and therefore unconstitutional."[68] While the case did not involve surveillance of foreign powers or their agents, the depth and force of this bold insinuation that no national security exception should exist provided the executive branch and Congress with a substantial basis for reconsidering the state of the law in this area. The plurality opinion also provided a point-by-point rebuttal of the entire array of arguments the executive branch had relied upon for years to establish the legality and reasonableness of warrantless surveillance.[69]

In concluding its discussion, the *Zweibon* court underscored the potential for flexibility as to the scope, standards, and approval periods that could be constitutionally applied by a court engaged in a prior review.[70] This portion of the opinion anticipated many of the key elements addressed in the Foreign Intelligence Surveillance Act.

---

[64] *Id.* at 916. The court noted that FISA had been enacted while the case was pending and that such activities would be subject to prior judicial review in the future. *Id.* at 914 n.4.

[65] 516 F.2d 594 (D.C. Cir. 1975), *cert. denied*, 425 U.S. 944 (1976).

[66] *Id.* at 600.

[67] *Id.* at 614.

[68] *Id.* at 614, (emphasis added). For a more detailed discussion of the sweeping statement, see *id.* at 655-58.

[69] *Id.* at 615-27, 633-51.

[70] *Id.* at 667-70.

III. The Foreign Intelligence Surveillance Act Is Born

A. *Development of FISA*

1. The Congressional Challenge to Executive Pre-eminence

By the mid-1970s, the law concerning national security-related electronic surveillance remained obscure, ambiguous and inconclusive despite almost fifty years of intermittent judicial and congressional attention and the practice of nine presidential administrations. The majority of the courts that had examined the legality of these matters seemed to focus as much or more on the purpose of the surveillance as on the underlying authority and nature of the subject. In *Keith,* the Supreme Court had invited Congress to develop standards for national security-related electronic surveillance that differed from those required for law enforcement surveillance in the 1968 Omnibus Act. These standards, according to the Court, could include less precise findings of probable cause and even a specially designed court to authorize sensitive activities.[71]

In an effort to ensure that its surveillance activities would be found reasonable if examined subsequently, the Executive unilaterally adopted warrantless electronic surveillance standards and procedures without specific congressional or judicial guidance. Such surveillance was to be limited to cases where the targets were foreign powers or their agents and where the purpose was to obtain foreign intelligence or counter-intelligence information. In addition, the scope of the intrusion and the use to which its fruits could be put would be carefully limited.[72]

The congressional mood at this time was one of antagonism toward the Executive because of Watergate and the disclosures in 1975 and 1976 of a broad range of perceived abuses of authority, especially in the area of intelligence and national security-related activities. The inquiries of the "Church Committee" into the activities of the intelligence agencies of the United States had uncovered far-ranging infringements upon individual privacy interests through the unfettered use of electronic surveillance and other intelligence collection techniques.[73] Of

---

[71] 407 U.S. at 322-23.

[72] *See Electronic Surveillance Hearings, supra* note 3, at 77 (statement by Attorney General Levi).

[73] *See* Final Report of the Senate Select Comm. to Study Governmental Operations With Respect to Intelligence Activities, Intelligence Activities and the Rights of Americans, Book II, S. Rep. No. 755, 94th Cong., 2d Sess., 19, 139, 151-53, 169-70, 183-92, 198-202, 290 (1976) [hereinafter Church Committee Report].

particular concern were instances where warrantless electronic surveillance had been used against United States citizens who were not readily identifiable as reasonable sources of foreign intelligence information, who appeared to pose little threat to the national security, and who were not alleged to be involved in any criminal activity.[74] The Church Committee reported that the abuses of executive discretion resulted from the absence of clear congressional or judicial standards and the unsettled state of the law in this area.[75]

The Church Committee's final recommendations included a general disclaimer of any inherent authority on the part of the President or the intelligence agencies to "violate the law" by engaging in, among other things, warrantless electronic surveillance.[76] The Committee recommendations further urged a statutory framework restricting electronic surveillance for intelligence purposes within the United States to that conducted by the FBI pursuant to a judicial warrant.[77] The report also included recommendations that use of these techniques against Americans abroad also be permitted only pursuant to a judicial warrant.[78]

By 1978, the recommendations embodied in the Church Committee report appeared to have persuaded many in Congress of the need to regulate electronic surveillance for national security purposes.[79] In par-

---

[74] *See id.* at 5.

[75]

> Congress and the Supreme Court have both addressed the legal issues raised by electronic surveillance, but the law has been riddled with gaps and exceptions. The Executive branch has been able to apply vague standards for the use of this technique to particular cases as it has seen fit, and, in the case of [National Security Agency] monitoring, the standards and procedures for the use of electronic surveillance were not applied at all.

Id. at 186-87.

[76] *Id.* at 297.

[77] *See id.* at 299, 302; *see also id.* at 325, 327-28 (urging that surveillance be conducted only pursuant to a judicial warrant).

[78] *Id.* at 305-06, 308-09.

[79] The difficulties obstructing the judicial construction of a reasonable framework for national security activities were aptly described by the House Permanent Select Committee on Intelligence:

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

ticular, Congress was urged to act and adopt a legislative framework that would remove electronic surveillance for national security purposes from the sole discretion of the Executive.[80]

Among the earliest and most serious issues confronting Congress was the threshold question of whether it was permissible to involve federal judges in approving requests for electronic surveillance conducted for national security purposes. These fears were alleviated by a legal analysis completed at the request of Congress which concluded that "there is every reason to believe that Congress may constitutionally confer such authority."[81] The conclusion was based on three independent premises: that a surveillance approval constitutes a case or controversy arising under Article III of the Constitution; that similar other functions such as naturalization and bankruptcy proceedings had been previously imposed upon the courts; and that judicial supervision of governmental intrusions into individual privacy was consistent with the drafters' intent in delineating judicial power in Article III of the Constitution.[82]

2. Cooperation and Compromise

Proponents of national security electronic surveillance legislation received their greatest encouragement from Attorneys General William Saxbe and Edward Levi. These officials agreed to work with the Senate to establish judicial regulation of such surveillance that would respect civil liberties yet facilitate the acquisition of necessary intelligence information.[83]

---

case law which adequately balances the rights of privacy and national security.

H.R. REP. No. 1283, 95th Cong., 2d Sess., pt. 1, at 21-22 (1978).

[80] *See id.*

[81] *See Constitutional Validity of a Statutory Provision Vesting Authority in the United States District Courts to Consider and Issue Orders Approving the Interception of Wire and/or Oral Communications for the Purposes of Gathering Foreign Intelligence Information: Presence of a Case or Controversy*, Congressional Research Service, American Law Division, 1 (1975).

[82] *Id.* While the Supreme Court invalidated the Bankruptcy Act of 1978 in Northern Pipeline Construction Co. v. Marathon Pipeline Co., 458 U.S. 50 (1982) for violating separation of powers principles, the formalistic conception of Justice Brennan's plurality opinion regarding Article III did not affect the analysis in the above report. Furthermore, the Court has moved away from the Brennan approach towards a functional analysis in Thomas v. Union Carbide Agricultural Products Co., 473 U.S. 568 (1985) and in Commodity Futures Trading Commission v. Schor, 106 S. Ct. 3245 (1986). The initial analysis permitting Article III judges to be involved with surveillance procedures remains valid.

[83] *See Hearings on S. 743, S. 1888, S. 3197 before Senate Judiciary Comm. Subcomm. on Criminal Laws and Procedures*, 94th Cong., 2d Sess., 71 (March 29-30, 1976).

Another sizable step forward occurred when, on March 23, 1976, President Ford transmitted a bill to the Senate along with a letter urging its enactment.[84] The transmittal letter explained that the proposal would enable the Government to collect necessary foreign intelligence but assured the public that national security electronic surveillance would occur only in circumstances demonstrating an overriding national interest, and would conform to standards and procedures that "protect against abuse."[85] This bill drew upon the Supreme Court's suggestion in *Keith* that Congress could provide specialized warrants consistent with the varying governmental and private interests affected. It included a warrant standard permitting the interception of wire or oral communications upon a finding of probable cause that the "target" was an agent of a foreign power and was engaged in clandestine intelligence activities, sabotage, or terrorism at the direction of that power.[86]

President Ford's proposal also preserved the constitutional power of the President to authorize surveillance in circumstances that would not be covered by the bill and where such surveillance was deemed necessary for the national defense purposes that had been described in the 1968 Omnibus Act.[87]

For the next two years, substantial discussion centered upon the question of reserved presidential authority and the issue of whether a "criminal standard," i.e., an additional requirement that no American be a target unless that individual's activities can be shown to constitute a violation of United States criminal law, should be included in the bill. The proponents of this requirement argued that electronic surveillance should be limited to cases involving violations of criminal law[88] since it

---

[84] *See Hearings on S. 743, S. 1888, S. 3197 Before the Subcomm. on Criminal Laws and Procedures of the Senate Judiciary Comm.*, 94th Cong., 2d Sess. 71 (1976) (statement of Sen. Kennedy reading prepared statement of Sen. Nelson) [hereinafter *Criminal Hearings*].

[85] *See* Letter to the Speaker of the House and the President of the Senate Transmitting Proposed Legislation on the Use of Electronic Surveillance To Obtain Foreign Intelligence Information (March 23, 1976), 1 PUB. PAPERS 793 (1979) (papers of Gerald R. Ford).

[86] *See id.* at 794.

[87] *Hearings on s. 743, S. 1888, S. 3197 before Senate Judiciary Comm. Subcomm. on Criminal Laws and Procedures, supra* note 85, at 124 (citing § 2511(3)).

[88] *See Hearings on the FISA of 1977, H.R. 5794, H.R. 9745, H.R. 7308 and H.R. 5632, Before the House Perm. Select Comm. on Intelligence Subcomm. on Legislation on the FISA of 1977*, 95th Cong., 2d Sess. 92 (1978) [hereinafter *House Hearings on the FISA of 1977*] (testimony of John Shattuck, Executive Director, Washington Office of the ACLU) ("if the wiretap standard is too low . . . Congress could end up . . . authorizing, rather than curtailing, intelligence agency abuses."); *see also id.* at 9-11 (prepared statement of Attorney General Griffin Bell), 80-82 (prepared statements of John Shattuck and Jerry J. Berman, Legislative Counsel to the ACLU), 101-102 (testimony of Louis H. Pollack, Dean of the University of Pennsylvania Law

is generally intrusive and inherently results in the acquisition of many irrelevant communications.

These two elements, the standard for targeting Americans and the status of the President's inherent authority, formed the core of subsequent legislative deliberations.[89] Other persistent but less contentious issues included, in addition to whether authorizing such activities was a proper role for the federal courts, the treatment afforded aliens in the United States and whether the bill should be extended to warrantless surveillance of Americans overseas.

Hearings on the Ford proposal continued through 1976. At the same time, Senator Kennedy introduced a bill that built upon the prior year's legislation, but differed in several meaningful respects from the Ford bill. It specifically repealed the provision in the 1968 Omnibus Act addressing constitutional Presidential authority and was intended to eliminate, or at least limit, inherent presidential authority in this area. The Kennedy bill also required a warrant for the interception of international communications to or from targeted Americans in the United States.[90] The provisions that allowed targeting of Americans who had committed no violation of federal criminal law remained the most serious issue in the hearings that followed.[91]

The Carter Administration supported such legislation in principle and continued to work with Congress to develop an acceptable proposal.[92] The bills with the greatest support required a judicial warrant prior to surveillance. At the same time, there continued to be sentiment for a system, such as that proposed by Congressman McClory, that would create statutory, non-judicial authority for an executive branch approval procedure.[93] Such a system was based upon the assertion that judicial involvement in the foreign intelligence area was inappropriate,

---

School), 195 (prepared statement of Rep. Robert F. Drinan).

[89] *See generally, Hearings on S. 3197 Before the Senate Select Comm. on Intelligence Subcomm. on Intelligence and the Rights of Americans*, 94th Cong., 2d Sess. (1976).

[90] *See House Hearings on the FISA of 1977*, *supra* note 90, at 8-9; *Foreign Intelligence Surveillance Act of 1978: Hearings on S. 1566 Before the Subcomm. on Intelligence and the Rights of Americans of the Senate Select Comm. on Intelligence*, 95th Cong., 2d Sess. 13 (1977-78) [hereinafter *Senate Intelligence Committee hearings on the FISA of 1978*] (prepared statement of Attorney General Griffin Bell); *Foreign Intelligence Surveillance Act of 1977: Hearings on S. 1566 Before the Subcomm. on Criminal Laws and Procedures of the Senate Judiciary Comm.*, 95th Cong., 1st Sess. 14 (1977) [hereinafter *Senate Judiciary Comm. Hearings on the FISA of 1977*] (statement of Attorney General Griffin Bell).

[91] *See Criminal Hearings*, *supra* note 86, at 12.

[92] *See House Hearings on the FISA of 1977*, *supra* note 90, at 12 (prepared statement of Attorney General Griffin Bell).

[93] *See id.* at 275; *id.* at 219-22 (testimony of the Hon. Laurence Silberman).

and would have required certification by the President, Attorney General, and the National Security Advisor to the President, or other senior officials. The certification would ensure that the target of the surveillance was an agent of a foreign power and that the other elements required by the bill were present.[94]

The House Permanent Select Committee on Intelligence examined the alternatives and, after extensive hearings, recommended that the House enact the House version of the Kennedy bill.[95] The Senate Select Committee on Intelligence had earlier reported favorably on the Senate version.[96] By this time, both bills had been modified to include a "quasi-criminal" targeting standard, i.e., Americans could be the targets of national security electronic surveillance only if their conduct, in addition to being of foreign intelligence interest, held the potential for violating a criminal law of the United States.[97] Further, the Justice Department had analyzed the law and found a substantial basis for providing different standards for targeting aliens representing foreign governments in the United States.[98] This conclusion was based upon the premise that, to the extent these persons enjoy diplomatic immunity and are not generally subject to the strictures of our laws, they do not enjoy the same levels of protection under our laws, specifically the Fourth Amendment.[99]

After the Senate and House Conference, Congress passed the resulting bill, and it was signed into law by President Carter in October 1978.[100]

B. *The Fruit of Interbranch Cooperation: FISA*

The Foreign Intelligence Surveillance Act is intended to provide the exclusive means of authorizing various types of electronic surveillance activities for national security purposes, including:

(1) deliberate interception of the contents of international radio or wire communications to or from a particular United States person in the United States in circumstances where that person has a reasonable expectation of privacy and a warrant would be required if the interception were undertaken for law enforcement purposes;

---

[94] *See* H.R. REP. NO. 1283, PT. 1, 95th Cong., 2d Sess., pt. 1, at 4-5 (1978).

[95] *See id.* at 2.

[96] *See generally*, S. REP. NO. 701, 95th Cong., 2d Sess. (1978).

[97] *See House Hearings on the FISA of 1977, supra* note 90, at 195; H.R. REP. NO. 1283, *supra* note 22, at 3, 62.

[98] *See House Hearings on the FISA of 1977, supra* note 90, at 23.

[99] *See id.* at 25.

[100] *See* Foreign Intelligence Surveillance Act of 1978 - Statement on Signing S. 1566 Into Law, 2 PUBLIC PAPERS 1853 (Oct. 25, 1978) (papers of James E. Carter).

(2) deliberate interception of the contents of a wholly domestic radio communication, and the installation or use of any monitoring device (such as a television camera or pen register) to acquire information about a person's activities other than the contents of communications, when there is a reasonable expectation of privacy and a warrant would be required if the interception or monitoring were undertaken for law enforcement purposes;

(3) interception in the United States of the contents of a wire communication to or from any person in the United States without the consent of a party to the communication.[101]

Such activities must be authorized in advance by one of seven federal district court judges designated by the Chief Justice of the Supreme Court as members of the Foreign Intelligence Surveillance Court (FISC) and at least one of whom is a member of a federal district court in the Washington, D.C. area.[102] The government presents applications for warrants to the FISC judges in *in camera,* ex parte proceedings conducted under physical security measures designed to protect sensitive national security information.[103] The Chief Justice also designates three federal appeals court judges to review government appeals in instances in which FISC judges have denied applications for warrants.[104]

All applications to the FISC require advance approval from the Attorney General.[105] A FISC judge may approve applications upon a finding that the target is a foreign power (i.e., foreign government, faction, terrorist or political group, or organization controlled by a foreign government), or an agent of a foreign power (i.e., a non-resident alien who is an officer, employee, or agent of a foreign power, and United States persons whose activities on behalf of foreign powers may involve criminal acts relating to intelligence or terrorist operations).[106] The term "United States person" is used to identify persons and entities that are entitled to greater protection under the Act and includes any United States citizen, permanent resident alien, groups composed largely of such persons, and United States corporations.[107]

The FISC judge must find the location at which the surveillance is directed will be used by the targeted foreign power or agent, and that procedures proposed by the government in each case will adequately

---

[101] *See* Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801(f) (1982 & Supp. 1984).

[102] *Id.* at § 1803 (a).

[103] *Id.* at §§ 1804(a),1805(a), 1803(c).

[104] *See id.* at § 1803(b).

[105] *Id.* at §§ 1804(a), 1805(a)(3).

[106] *Id.* at §§ 1801(a), (b), 1805(a)(3).

[107] *Id.* at § 1801(i).

minimize the acquisition, retention, and dissemination of information concerning unconsenting United States persons, while preserving the government's ability to obtain the intelligence it seeks.[108] Applications to the FISC must be accompanied by certifications from senior government officials that the information sought "relates to" or, if it concerns a United States person, "is necessary to" United States national defense or foreign affairs, or the ability to the United States to protect against grave hostile acts, terrorism, sabotage, or clandestine intelligence activities of a foreign power.[109] If the FISC judge is satisfied that the relevant standards of the Act have been met, electronic surveillance may be approved for up to ninety days or a year, depending upon the nature of the target.[110] Renewal applications are subject to the same standards.[111]

Although the Attorney General must approve and make certain findings, there is no requirement of a FISC order when surveillance is directed solely at communications among or between foreign powers or is targeted at property under the "open and exclusive" control of a foreign power, where the circumstances indicate it is highly unlikely that communications of a United States person will be acquired.[112] The only other exceptions from the requirement for a FISC order are emergencies, where the Attorney General may approve warrantless surveillance for up to twenty-four hours while FISC approval is pursued, and specified types of testing, training, and communications security activities.[113]

The Act also contains detailed provisions specifying the requirements and procedures mandated when information obtained from surveillance activities is intended to be used in criminal or other proceedings.[114] Barring such situations or an emergency surveillance approval by the Attorney General that is subsequently rejected by the FISC, however, there is no requirement to give notice to any target concerning the fact that the government has conducted such surveillance.[115]

---

[108] *Id.* at §§ 1804(a)(4)(B), (5), 1801(h).

[109] *Id.* §§ 1804(a)(7), 1801(e)(2). Six hypothetical situations supplied by Attorney General Griffin Bell during congressional proceedings illustrate the potential difficulties in determining whether warrants for electronic surveillance should be pursued under the 1968 Omnibus Act or FISA. *See Judiciary Comm. Hearings on the FISA of 1977, supra* note 90, at 8-10 (letter to Senator Abourezk from Attorney General Griffin Bell dated June 28, 1977). *See also Senate Intelligence Committee Hearings on the FISA of 1978, supra* note 92, at 119-21 (containing the six hypothetical cases submitted by Attorney General Griffin Bell).

[110] 50 U.S.C. § 1805(d).

[111] *Id.*

[112] *Id.* at §§ 1802(a)(1)(A), (B).

[113] *Id.* at §§ 1805(e), (f).

[114] *Id.* at § 1806.

[115] *Id.* at § 1806(j).

IV. FISA IMPLEMENTATION AND CONSTITUTIONALITY

The Act requires semi-annual reports from the Attorney General to the Senate and House Intelligence Committees and those committees were required to report to their respective houses of Congress annually concerning the implementation of the Act during its first five years.[116] The Attorney General's reports[117] indicate that the FISC has reviewed in the following number of applications and that no government request for electronic surveillance has been denied by the court during its first ten years of existence:

		Applications	Orders[118]
May 1979[119] - December 1979		199	207
January 1980 - December 1980		319	322
January 1981 - December 1981		431	433
January 1982 - December 1982		473	475
January 1983 - December 1983		549	549

[116] *Id.* at §§ 1808(a), (b).

[117] *See generally* SENATE SELECT COMM. ON INTELLIGENCE, IMPLEMENTATION OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, S. REP. NO. 379, 96th Cong. 1st Sess. (1979) [hereinafter SSCI FISA REP.]; S. REP. NO. 1017, 96th Cong. 2d Sess. (1980); S. REP. NO. 280, 97th Cong., 1st Sess. (1981); S. REP. NO. 691, 97th Cong., 2d Sess. (1982); S. REP. NO. 660, 98th Cong., 2d Sess. (1984); HOUSE PERMANENT SELECT COMM. ON INTELLIGENCE, IMPLEMENTATION OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, H. R. Rep. No. 558, 96th Cong., 1st Sess. (1979) [hereinafter HPSCI FISA REP.]; H.R. REP. NO. 1466, 96th Cong., 2d Sess. (1980); H. R. REP. NO. 318, 97th Cong., 1st Sess. (1981); H.R. REP. NO. 974, 97th Cong., 2d Sess. (1982); H. R. REP. NO. 738, 98th Cong., 2d Sess. (1984). In addition, see the following letters on file with the University of Pennsylvania Law Review; letter from Attorney General Benjamin R. Civiletti to the Speaker of the U.S. House of Representatives (April 20, 1980); letter from Attorney General William French Smith to the Speaker of the U.S. House of Representatives (April 22, 1981); letter from Attorney General William French Smith to William E. Foley, Director, Administrative Office of the United States Courts (April 15, 1982); letter from Edward C. Schmults, Acting Attorney General to William E. Foley, Director, Administrative Office of the United States Courts (April 4, 1983); letter from Attorney General William French Smith to William E. Foley, Director, Administrative Office of the United States Courts (March 6, 1984); letters from Attorney General Edwin Meese III to William E. Foley, Director, Administrative Office of the United States Courts (March 6, 1985, March 5, 1986, March 24, 1987, March 30, 1988). The reports and letters verify that no government request for electronic surveillance has been denied by the court.

[118] The number of orders may exceed the number of applications because surveillance of more than one location or use of more than one surveillance technique may be requested in a single order. *See* H.R. REP. NO. 738, 98th Cong., 2d. Sess. 4 n.5 (1984).

[119] The legislation was enacted with the expectation of a delay between its enactment and implementation. It states that the act was effective immediately except that "electronic surveillance approved by the Attorney General . . . shall not be deemed unlawful for failure to follow the procedures of this Act, if that surveillance is terminated or an order approving [it] . . . is obtained . . . within 90 days following designation of the first judge." *See* Pub. L. 95-511, *supra* note 1, at Title III.

January 1984 - December 1984	635	635
January 1985 - December 1985	573	573
January 1986 - December 1986	587	587
January 1987 - December 1987	512	512[120]
Totals	4278	4293

Thus, in over four thousand matters involving electronic surveillance using various techniques directed at various types of targets in various circumstances, the FISC saw fit to deny no government request.[121] As is explained in more detail in the next section of this commentary, the only instance in which the FISC has denied a government application occurred when, at the government's own urging, the FISC reversed itself and determined that it had no jurisdiction to authorize physical searches for intelligence purposes.

Proponents of FISA argue that the lack of a denial demonstrates the careful consideration and judgment exercised by the executive branch in reviewing and preparing applications for submission to the FISC, and that only cases that satisfactorily meet the statutory standards are brought before the Court.[122] Opponents argue that the secrecy that surrounds the FISC prevents a determination of whether these figures indicate instead that the FISC has become a captive of the national security establishment and serves only to encourage executive officials, now protected by judicial approval, to conduct activities that would otherwise never have been proposed.[123]

---

[120] The decrease in annual totals does not necessarily indicate a decrease in the use of FISA but may be traced to a number of factors such as consolidation of surveillance requests regarding similar targets, a reduction in the number of available targets, changes in government priorities, a lack of adequate resources, or even technical implementing difficulties.

[121] There appears to have been at least one instance in which a FISC judge modified a government request, authorizing the government to conduct a type of activity that had not been requested. *See* S. REP. 660, 98th Cong., 2d Sess. 8 (1984). *See also* Schwartz, *Oversight of Minimization Compliance Under the Foreign Intelligence Surveillance Act: How the Watchdogs Are Doing Their Jobs*, 12 RUTGERS L.J. 405, 441 n.212 (1981).

[122] *See, e.g., Foreign Intelligence Surveillance Act: Oversight Hearings Before the Subcomm. on Courts, Civil Liberties, and the Administration of Justice of the House Comm. on the Judiciary*, 98th Cong., 1st Sess. 6 (1983) (testimony of Mary C. Lawton, Counsel for Intelligence Policy, Department of Justice, stating, "[t]o date, the court has not rejected a single application. We are proud of that record."). The chairman of the subcommittee went so far as to suggest that a flawed application could be submitted merely to obtain a FISC denial and dispel the court's "rubber stamp" image. *Id.*

[123] *Id.* at 27 (testimony of Mark Lynch, Attorney, ACLU). These fears should be alleviated somewhat by the fact that all the district and circuit courts that have conducted independent reviews of FISC authorizations have determined them to have been lawful. *See id.* at 6-7 (testimony of Mary C. Lawton); *see also infra* notes 127-53 and accompanying text.

The constitutional issues that were debated during consideration of the various bills that preceded the enactment of FISA have persisted. These issues include whether the Congress has the power to limit or regulate executive authority that was long thought to be inherent and constitutionally based. Another area of dispute concerns the extent to which the fourth amendment requires procedures patterned on those embodied in the 1968 Omnibus Act rather than those adopted in FISA which, among other differences, allows some forms of warrantless surveillance and requires no notice to the targets. There continues to be concern over whether surveillance should be authorized, particularly against a United States person, when there is no finding of probable cause to believe a crime is being, has been, or is about to be (as opposed to the FISA standard of "may be,") committed and that evidence of criminal activity will be obtained. Also, the distinctions and differing levels of protection afforded aliens, as opposed to United States persons, in the United States have continued to be debated.[124]

Additional questions continue to revolve around the government's authority under the statute to exclude a criminal defendant and obtain an ex parte, *in camera* hearing on any motion to suppress information acquired under FISA. Further, the entire FISA framework has been challenged as overly broad, far too generalized, and unreasonable in the burdens it imposes on individual privacy interests in favor of the government and in the name of national security. Finally, the nature of the judiciary is subject to challenge on the grounds that federal judges lack the jurisdiction to perform the function FISA gives them and that they lack the competence to intrude into the President's foreign policy domain.[125]

These questions — the faithfulness of FISA implementation by the Executive and the FISC, as well as the constitutional validity of the statutory framework itself — have undergone repeated scrutiny by the federal courts, generally in the context of terrorism and espionage pros-

---

[124] *See, e.g.*, Note, *The Foreign Intelligence Surveillance Act: Legislating a Judicial Role in National Security Surveillance*, 78 MICH. L. REV. 1116, 1135-50 (1980) (discussing the separation of powers issues that FISA raises); Note, *The Foreign Intelligence Surveillance Act of 1978*, 13 VAND. J. TRANSNAT'L L. 719, 747-59 (1980) (discussing whether the legislative branch is overstepping its boundaries by enacting FISA and whether FISA violates the fourth amendment); *see also infra* notes 127-134 and accompanying text; Jachnycky & Kornblum, *America's Secret Court: Listening in on Espionage and Terrorism*, 24 JUDGES' J., 15, 17 (1985) (discussing cases that have upheld the constitutionality of FISA against challenges that the FISA court was not created in accordance with Article II of the Constitution, and that FISA violates the due process clause of the fifth amendment).

[125] *See* Jachnycky & Kornblum, *supra* note 124, at 16.

ecutions, during the ten years since FISA became law.[126] The legal arguments that have been made in these cases in opposition to surveillance activities authorized under FISA have fallen into the same general categories — the basic constitutionality under the Fourth and Fifth Amendments of FISA's targeting and procedural standards, the nature and competency of the FISA Court, and basic compliance with the requirements of the statute in terms of the actual purpose of the surveillance and the sufficiency of the minimization procedures that are utilized to protect the privacy interests of communicants. These arguments, and the judicial response to them, are best illustrated by reviewing the opinion in *United States v. Duggan*.[127]

In *Duggan*, the defendants had been convicted of violating various firearms and munitions statutes on behalf of the Provisional Irish Republican Army. At trial, motions to suppress evidence obtained through a FISA surveillance were denied.[128] The trial court had satisfied itself as to the propriety of the surveillance on an ex parte, *in camera* basis following the filing of an Affidavit and Claim of Privilege by Acting Attorney General Edward Schmults.[129] On appeal, the defendants asserted a broad range of attacks on FISA.

At the constitutional level, they contended that the statutory stan-

---

[126] The following cases have involved public review of FISA surveillance since FISA was enacted: United States v. Posey, No. 87-5297, slip op. (9th Cir. Jan. 9, 1989); In Re: Grand Jury v. (Under Seal), No. 88-5610 (4th Cir. filed Sept. 14, 1988); United States v. Pelton, 835 F.2d 1067 (4th Cir. 1987), *cert. denied,* 108 S. Ct. 1741 (1988); United States v. Badia, 827 F. 2d 1458 (11th Cir. 1987) *cert. denied*, 108 S. Ct. 1115 (1988); United States v. Ott, 827 F. 2d 473 (9th Cir. 1987); United States v. Cavanaugh, 807 F.2d 787 (9th Cir. 1987); *In re* Kevork, 788 F.2d 566 (9th Cir. 1986); United States v. Duggan, 743 F. 2d 59 (2d Cir. 1984); United States v. Belfield, 692 F. 2d 141 (D.C. Cir. 1982); United States v. Psinakis, CR-86-1064-RHS (N.D. Cal. 1988) (upheld without opinion): United States v. Hawamda, Crim. No. 88-168-A (E.D. Va. filed Sept. 25, 1988); United States v. Davies, 86-1003-SAW (N.D. Cal. 1989) (upheld without opinion): United States v. Chin, Crim. No. 85-263-A (E.D. Va. filed Jan. 29, 1986); United States v. Ogorodnikova (C.D. Cal. 1985) (upheld without an opinion); United States v. Miller, CR No. 84-972(A) -KN (C.D. Cal. 1985) (pending at 9th Cir.); United States v. Harper, CR 83-0770-SC (N.D. Cal. 1984); United States v. Zehe, No. 83-296-N (D. Mass. filed Feb. 15, 1984); United States v. Horton, (E.D. Va. 1983) (upheld without opinion); United States v. Falvey, 540 F. Supp. 1306 (E.D.N.Y. 1982); United States v. Zacharski, No. CR 81-679-Kn (C.D. Cal. filed Sept. 23, 1981); United States v. Hovsepian, No. CR 82-917-MRP (C.D. Cal. filed Jan. 25, 1985), *aff'd sub nom.* United States v. Sarkissian, 841 F. 2d 959 (9th Cir. 1988). In three other cases, FISA issues were involved but the defendants were exchanged for individuals held behind the Iron Curtain before the issues were decided. *See* United States v. Kostadinov, 83-CR-616 VLB (S.D.N.Y. 1984); United States v. Koecher, 84-CR-1001 (S.D.N.Y. 1984); United States v. Michelson, CR 84-00578 (E.D.N.Y. 1984).

[127] 743 F.2d 59 (2d Cir. 1984).

[128] *Id.* at 64-65.

[129] *Id.* at 67; *see also* United States v. Megahey, 553 F. Supp. 1180, 1196-97 (E.D.N.Y. 1982), *aff'd sub nom.* United States v. Duggan, 743 F.2d 59 (2d Cir. 1984).

dard for targeting individuals under FISA did not satisfy fourth amendment probable cause requirements and deprived individuals of due process and equal protection.[130] The Second Circuit concluded that the FISA concepts of national defense, national security, and foreign affairs were not overly vague and that the portions of FISA that related to these defendants were "plainly applicable . . . explicit, unequivocal, and clearly defined."[131] As for the claim that collecting foreign intelligence under FISA is unconstitutional because the fourth amendment requires there to be probable cause to believe a crime has been committed in all cases of government surveillance, the court retraced the history of judicial recognition of the substantially different interests involved in national security and criminal investigations.[132] After discussing the purposes of FISA, it concluded that the statutory procedures created a "constitutionally adequate balancing of the individual's Fourth Amendment rights against the nation's need to obtain intelligence information."[133]

Similarly, the appeals court did not believe that the differentiation between aliens and United States persons that is embodied in FISA violated equal protection principles.[134] Rather, this framework was viewed as an appropriate exercise of political judgment by the Congress and was rationally related to the purpose of protecting the United States against actions of foreign powers.[135]

The nature and competency of the FISC was challenged by alleging that vesting authority in judicial officers to determine "a political question," that is, whether a surveillance is necessary to acquire foreign intelligence relevant to the conduct of United States foreign affairs and combatting terrorism, is a violation of separation of powers principles.[136] The court responded that the determination was a traditional factual, not political, process and that the limited role of the FISC judges in ensuring that an executive branch certification that the surveillance is necessary is not "clearly erroneous" did not unduly involve the courts in foreign policy matters.[137] The district court had also rejected the argument that the establishment of the FISC violated the

---

[130] *Duggan*, 743 F.2d at 64-65.

[131] *Id.* at 71.

[132] *Id.* at 72-74.

[133] *Id.* at 73.

[134] *Id.* at 75.

[135] *Id.* at 75-76. Additional constitutionally-based assertions that the FISA procedures for ex parte, *in camera* review violate due process have met with a similar lack of success. *See, e.g.*, United States v. Belfield, 692 F.2d 141, 148-49 (D.C. Cir. 1982).

[136] *Duggan*, 743 F.2d at 74-75.

[137] *Id.*.

provisions of article III of the Constitution insofar as FISC proceedings are entirely ex parte, because federal judges are not appointed to the FISC for life and receive no additional compensation for their service in that capacity.[138]

Finally, the defendants asserted that the terms and conditions of FISA had not been satisfied in their case since the surveillance was part of a criminal, not national security, investigation.[139] While the appeals court recognized the requirement that the collection of foreign intelligence be "the primary objective" of a FISA surveillance, it also noted that the courts are intended to have a limited role in assessing the validity of the purpose asserted by the government in a particular case unless there is evidence of actual fraud on the court.[140] The mere collection of information that may later be useful as evidence in a criminal proceeding, even if foreseeable, does not undermine the legality of a FISA surveillance so long as there is a certified foreign intelligence purpose.[141] The court also noted that there is no requirement in FISA to identify all the persons whose communications might be acquired in the course of the surveillance of an appropriate target.[142] Additional minimization issues had been disposed of satisfactorily by the district court.[143]

A unique set of issues relating to FISA was raised in the case of *In re Kevork*.[144] The FISA electronic surveillance in Los Angeles that resulted in terrorism charges in the United States[145] also revealed a conspiracy to assassinate a Turkish official in Canada.[146] The three individuals who were indicted in Canada moved to suppress evidence obtained from the surveillance in the United States on the ground that FISA bars disclosure of information acquired under the Act for use in a foreign criminal proceeding.[147] A "commission," consisting of a United States Federal District Court Judge and an Ontario Supreme Court Justice, had been appointed by the District Court for the Central District of California and the Supreme Court of Ontario, respectively, to hear testimony and gather evidence.[148] The Attorney General authorized the production of information obtained through the FISA surveil-

---

[138] *Megahey*, 553 F. Supp. at 1196-97.
[139] *Duggan*, 743 F.2d at 76.
[140] *Id.* at 77.
[141] *Id.* at 78.
[142] *Id.* at 79.
[143] *Megahey*, 553 F. Supp. at 1195.
[144] 788 F.2d 566 (9th Cir. 1986).
[145] *See id.* at 568; United States v. Sarkissian, 841 F.2d 959 (9th Cir. 1988).
[146] *See In re* Kevork, 788 F.2d at 568.
[147] *Id.*
[148] *Id.*

lance and the three individuals were informed of the proposed use as required by FISA.[149]

The individuals argued that FISA only speaks to federal, state, or local criminal proceedings and that, absent express statutory authorization, the introduction of evidence produced by electronic surveillance was barred by Supreme Court decisions preceding FISA and the 1968 Omnibus Act.[150] The Ninth Circuit disagreed and found no indication the issue had ever been raised, not to mention decided, by the courts.[151] Furthermore, Congress clearly had contemplated dissemination to foreign governments of intelligence information acquired through FISA surveillance and there was no reason to believe its ultimate use in foreign judicial proceedings was intended to be barred. Thus, the suppression was denied.

Of course, despite the fact that the government has been successful to date in these cases and in countering every type of judicial challenge that has been raised to FISA, these issues will not be settled definitively unless and until the Supreme Court is afforded an opportunity to rule on the statute.[152] Nonetheless, it is significant that the fundamental constitutionality of the FISA process, the integrity with which it is being implemented, and the role of the FISC have withstood substantial judicial scrutiny. This is not to say that there has been no controversy regarding the implementation of FISA or that the statute could not be improved by amendment in light of experience and changing circumstances.

---

[149] *Id.*; 50 U.S.C. §§ 1806(c), (e) (1982).

[150] *In re* Kevork, 788 F.2d at 570. The appellants supported this contention by citing Berger v. New York, 388 U.S. 41 (1967) and Nardone v. United States, 308 U.S. 338 (1939). *Id.*

[151] *In re* Kevork, 788 F.2d at 570.

[152] *Id.* Several other cases involving examination of issues raised in conjunction with FISA surveillances are also noteworthy. In United States v. Hovsepian, CR 82-917-MRP (C.D. Cal. filed Jan. 25, 1985), for example, the District Court upheld the use of automatic tape recorders instead of more selective human monitors because of the likelihood the targets would use foreign or coded language. *In Re*: Grand Jury v. (Under Seal), No. 88-5610 (4th Cir. filed Sept. 14, 1988), concluded that a grand jury is not a "proceeding" requiring notice to witnesses of FISA surveillance. In United States v. Chin, Crim. No. 85-263-A (E.D. Va. filed Jan. 29, 1986), the same judge who applied the primary purpose test in the context of pre-FISA warrantless foreign intelligence surveillance in United States v. Truong, 629 F.2d 908, 912-13 (4th Cir. 1980), applied a similar mode of analysis to surveillance under FISA. In United States v. Hawamda, Crim. No. 88-168-A (E.D. Va. filed Sept. 15, 1988), the same judge upheld the legality of both a domestic FISA and non-FISA overseas electronic surveillance for national security purposes.

V. The Foreign Intelligence Surveillance Court and Physical Searches

During the debate over FISA, there were those who argued that the creation of the FISC would blur the constitutional lines of responsibility in the area of national security activities, would encourage the executive branch to undertake activities that might otherwise be inhibited, and would create a judicial entity that would necessarily become a captive of better informed and more experienced executive branch officials.[153] Those who voiced these concerns were able to assert vindication in late 1980 when the Justice Department disclosed that Attorney General Benjamin Civiletti had determined that requests for Attorney General approval of national security-related physical searches should be brought to the FISC for judicial review in cases where such review would not frustrate national security interests. This review would be sought even though the Attorney General continued to believe that the President retained the constitutional authority to approve such searches without judicial review.[154]

The requests for FISC approval of physical searches for national security purposes were patterned upon the procedures for electronic surveillance under FISA and represented the first time that such matters had been submitted for prior judicial review.[155] The premise for the Attorney General's decision was that the FISC provided a judicial forum with the security and expertise necessary for the review of such matters.[156] Since FISA clearly does not provide the requisite jurisdiction, the Justice Department argued that the FISC judges drew authority to review and approve physical searches for national security purposes directly from their inherent constitutional power as federal judges to ensure the integrity of the judicial process and to protect the fourth amendment interests of the subjects of such searches, and from the All Writs Act.[157] In 1980, the Department sought FISC approval of three physical searches, and in each case the FISC judges granted it.[158]

---

[153] *See, e.g., Hearings on the Foreign Intelligence Surveillance Act of 1977 Before the Subcomm. on Legislation of the House Permt. Select Comm. on Intelligence*, 95th Cong., 2d Sess. 3-5, 26-31, 125, 213-15, 226 (1978).

[154] *See* Memorandum from Kenneth C. Bass III, Counsel for Intelligence Policy, U.S. Department of Justice, to FBI Director William H. Webster, Oct. 14, 1980, *reprinted in* HPSCI FISA Rep. 1466, *supra* note 117, at 8-16.

[155] *See id.* at 8-9.

[156] *See id.* at 14-16.

[157] *Id.*; 28 U.S.C. § 1345 (1982) ("Except as otherwise provided by an Act of Congress, the district courts shall have original jurisdiction of all civil actions, suits or proceedings commenced by the United States, or by any agency or officer thereof expressly authorized to sue by Act of Congress.").

[158] *See* SSCI FISA Rep. 660, *supra* note 117, at 19 n.12.

Both congressional intelligence committees expressed concern and reservations when this use of the FISC was reported to them.[159] The FISC itself also harbored doubt as to its authority to review these matters, and directed the Clerk of the Court to develop a legal memorandum on the subject for the judges. That memorandum, issued after the three searches had been approved, concluded that neither the statutory language nor the legislative history gave any indication that the Congress intended to grant the FISC jurisdiction to authorize any activity that did not constitute "electronic surveillance" as defined in the statute.[160] The arguments concerning the inherent authority of federal judges and the authority conferred by the All Writs Act were dismissed as immaterial because all the sources that had been cited for this proposition were concerned with the powers of district court judges, not district court judges sitting as a special court with very carefully limited and defined jurisdiction.[161]

In the spring of 1981, following the transition to a new administration under President Ronald Reagan and Attorney General William French Smith, the Justice Department submitted another application to the FISC for authority to conduct a national security-related physical search.[162] This time, however, the Department sought to have the application rejected and accompanied it with a memorandum of law that argued that the FISC had no jurisdiction—explicit, implied, or inherent—to grant such an order.[163]

The Department argued that it was clear on the face of the statute that FISA contemplated only electronic surveillance applications, and that it was evident from the legislative history that physical searches were intended to be dealt with by Congress at a later time. Thus, the FISC had no express or implied jurisdiction over such matters.[164] As to inherent power, the memorandum argued that inherent constitutional authority to approve warrantless physical searches for national security purposes rests with the President, so there was no constitutional neces-

---

[159] *See* HPSCI FISA REP. 1466, *supra* note 117, at 5 (committee report), 25-26 (additional views of members Robinson, Ashbrook, McClory, Whitehurst, and Young); SSCI FISA REP. 1017, *supra* note 117, at 9-10.

[160] *See* Memorandum to Presiding Judge George L. Hart, Jr. from Robert S. Erdahl, October 30, 1980, *reprinted in* HPSCI FISA REP. 1466, *supra* note 117, at 17-24.

[161] *Id.* at 21-24.

[162] *See* SSCI FISA REP. 280, *supra* note 117.

[163] *See* Memorandum of Applicant, *In re* Application of the United States for an Order Authorizing the Physical Search of Nonresidential Premises and Personal Property (For. Intell. Surv. Ct., June 11, 1981), *reprinted in* SSCI FISA REP. 280, *supra* note 117, app. b. at 10-16 [hereinafter Physical Search Memorandum].

[164] *See id.* at 11.

sity for the FISC to act to protect fourth amendment interests.[165] Based on these arguments, the Justice Department asked the FISC in effect to reverse its previous decisions and reject any claim to jurisdiction in physical search cases.

Once again, the FISC agreed with the arguments of executive branch lawyers. Presiding Judge Hart issued an opinion on June 11, 1981, concluding that the Court does not have, and presumably never had, jurisdiction to approve physical searches. All the FISC judges concurred.[166] The opinion did not treat the constitutional issues that had been raised for accepting or rejecting jurisdiction over these activities, but relied solely on the language and purposes of FISA.[167] The Court found it significant that the Senate had considered extensive amendments to FISA in 1980 that would have expressly added physical searches to the FISC's jurisdiction and changed the Act's title to the "Foreign Intelligence Search and Surveillance Act." The amendments, contained in S. 2284, were not passed, however.[168]

Thus, the only denial by the FISC of any of the almost 4,300 requests made to it by the government during the first ten years of its existance was issued at the request of the executive branch.

VI. Looking Ahead — Possible Amendments to FISA

After less than a year of experience under FISA, the executive branch suggested that three amendments to the statute be considered.[169] Subsequently, two additional amendments were suggested by the Executive.[170] These amendments included:

—adding language to make clear that the term "agent of a foreign power" as used in FISA for targeting purposes includes individuals who hold both United States and foreign citizenship and are serving as senior officials in a foreign government;

—adding language to make clear that individuals who formerly held senior positions in a foreign government may also be targeted;

—extending to 48 hours the 24-hour period allowed in FISA for emergency surveillance while an application to the FISC is being prepared;

—authorizing an exception to the strict FISA limits on use and

---

[165] *Id.* at 14-15.

[166] *See* Physical Search Memorandum, *supra* note 163, at 16-19.

[167] *Id.*

[168] *See id.* at 18-19.

[169] *See* SSCI FISA Rep. 1017, *supra* note 117, at 6-9; HPSCI FISA Rep. 1466, *supra* note 117, at 4-5.

[170] *See* SSCI FISA Rep. 280, *supra* note 117, at 4-6.

dissemination of information acquired during training, testing, or efforts to protect against illegal electronic surveillance when the information indicates threats to human life or physical safety;

—adding language to make clear that the authority granted the Attorney General under FISA to approve electronic surveillance of foreign powers where there is no substantial likelihood of acquiring communications of United States persons includes authority to approve physical entry to premises as necessary to install, or remove listening devices.[171]

Congress has taken no action on these proposals. The Justice Department, however, reversed its earlier position and concluded some months subsequent to the transmittal of the proposed amendments that FISA in fact does authorize the Attorney General to approve physical entry when necessary to implement an electronic surveillance that the statute allows to be approved by the Attorney General alone.[172] That conclusion appears to have removed the need for this particular amendment and was based upon the reasoning of an earlier Supreme Court decision that utilized an analysis of not just the language, but also the structure and history, of a statute to find implied power where reasonably necessary to implement the statutory authority.[173]

The other proposed amendments have not been pursued with any vigor by the Executive or the Congress.[174] While this inaction seemingly indicates a lack of urgency, it is apparent that these proposals identify weaknesses in the law that may result in the loss of intelligence in particular circumstances and should be addressed before those circumstances arise again.

For example, it is possible that an individual who attained permanent resident alien status while living in the United States and then returned to his native country could become the Prime Minister or President of that country. If that person then visited the United States, FISA could be interpreted not to allow for surveillance of his communications unless a connection to the foreign country's intelligence activities could be established because the person would still be deemed a "United States person".[175] A foreign national who formerly held a senior position in a foreign country and is in the United States could be

---

[171] *Id.* at 4-8.

[172] *Id.*

[173] *See id.* (citing Dalia v. United States, 441 U.S. 238 (1979)).

[174] An additional possible amendment was noted in 1982, i.e., reducing the administrative burdens of FISA by allowing longer than 90 days for surveillance of foreign intelligence officers. *See* SSCI FISA REP. 691, *supra* note 117, at 5.

[175] *See* 50 U.S.C. § 1801(b) (1) (1982) (defining "agent of a foreign power" and "United States person").

insulated from FISA targeting unless there was evidence of current ties with a foreign political faction in that foreign country. This is a consequence of the current definition of "agent of a foreign power".[176]

FISA also must keep pace with the continuing explosion in communications technologies available both to law enforcement agencies and potential surveillance targets. FISA was drafted to take account of experience and technology developed between 1968 and 1978, but the decade since its passage has witnessed substantial technological changes that could require amendments to FISA in order to extend its privacy protections and to facilitate legitimate government interests that might otherwise be frustrated.[177] For instance, Congress saw a need in 1986 to make clear that the 1986 Omnibus Act applies to communications over fiber optic cable, as well as traditional wire transmissions.[178]

Another example is the increasing number of businesses and other organizations that are establishing private telephone systems for voice and data communications that are not part of a common carrier network.[179] Although the 1968 Omnibus Act has been amended to include such private systems within its requirements on interception,[180] FISA has not.[181]

In addition, it has been suggested that congressional and FISC oversight of Executive minimization practices under FISA should be enhanced.[182] The major difficulty with increasing the FISA Court's role in supervision of minimization is the additional burdens that would result. The judges are already devoting substantial amounts of time to reviewing five to six hundred applications each year and might be forced to abandon their regular district court positions if they must begin to travel around the country visiting various locations where FISA minimization takes place.[183] The additional workload would still be substantial if the records were required to be brought to the FISA judges and such a requirement would result in mammoth administra-

---

[176] *See id.*

[177] *Cf.* REPORT OF THE HOUSE JUDICIARY COMM. TO ACCOMPANY H.R. 4952, ELECTRONIC COMMUNICATIONS PRIVACY ACT OF 1986, H.R. REP. NO. 647, 99th Cong., 2d Sess. (1986) (technological change left new forms of telecommunication unprotected or uncertain as to protection. The 1968 Omnibus Act was enacted when most telecommunication consisted of voice communications over common carrier networks).

[178] *Id.*

[179] *See* H.R. REP. NO. 647, 99th Cong., 2d Sess. 32-33 (1986).

[180] *See* Pub. L. No. 99-508, 100 Stat. 1848 (1986) § 101(a) (1) (amending definition of "wire communication"), codified at 18 U.S.C. § 2510(1) (Supp. IV 1986).

[181] 50 U.S.C. § 1801 (l) (1982) (definition of "wire communication" that is limited to common carrier services).

[182] *See* Schwartz, *supra* note 121, at 433-90.

[183] This problem has been recognized even by one of the chief proponents of enhanced minimization oversight. *See id.* at 448-49.

tive and security problems for the implementing agencies. Similar difficulties would be created if an increased congressional role were required in monitoring minimization practices as well as the substantial separation of powers issues that arise whenever Congress seeks access to ongoing investigative files.[184] An oversight system based on random or sample reviews,[185] might not address fundamental concerns because it would provide no assurance of program-wide practices, and would require much negotiation between the overseers and the intelligence agencies concerning which files were to be reviewed and under what conditions.[186]

The public's confidence in the integrity of the process could be strengthened, however, by renewal of the statutory requirement, which expired after FISA's first five years, that the Senate and House intelligence committees issue annual reports regarding FISA's implementation. Apart from the episodic insights provided by judicial review and criminal proceedings, these reports comprise essentially the only public source of information regarding FISA practices and developments in the administrative and judicial areas.[187]

Perhaps the most promising area for possible amendment of FISA, however, is the recurring proposal to expand the FISC jurisdiction and provide specific statutory authorization for review and approval of physical searches for national security purposes. While the constitutional authority of the Executive to conduct these activities without judicial involvement appears to be well-established,[188] the same interests underlying enactment of FISA itself — protecting individual rights while facilitating legitimate government programs — would militate in favor of a statutory framework for physical searches.

It may be argued, as has been done in the past, that vesting authority in the FISC to approve the use of national security-related

---

[184] *See id.* at 483-90.

[185] *See id.* at 450-53 (recommending that the FISC conduct in-depth review of the products and use of products in a few randomly-selected surveillances and that counsel for the congressional committees be present to act as adversary of the intelligence agencies). In this latter regard, it is interesting to note that the procedures utilized by the Canadian Security Intelligence Service to obtain warrants for electronic surveillance for intelligence purposes include a requirement that a Canadian Justice Department attorney act as a "Devil's Advocate" to challenge such application. *See* Annual Report of the Security Intelligence Review Committee 1987-1988, at 15.

[186] Schwartz, however, proposed that the FISC have absolute discretion to examine any case it chooses. *See id.*

[187] *See* 50 U.S.C. § 1808(b) (1982). For a comprehensive listing of the published Senate and House reports, see *supra* note 117.

[188] *See* Brown & Cinquegrana, *Warrantless Physical Searches for Foreign Intelligence Purposes; Executive Order 12,333 and the Fourth Amendment*, 35 CATH. U. L. REV. 97, 107-37 (1985).

physical searches is an unconstitutional intrusion into presidential powers.[189] In response to this argument, it should be pointed out that FISA has worked to the Executive's advantage in the area of electronic surveillance despite similar concerns. The statutory foundation of these activities, and the judicial role in them, has enhanced rather than diminished executive power because it protects the government officials who are involved in these activities from civil or criminal liability and is indispensible in encouraging cooperation from the private sector individuals and entities that must be involved if these activities are to be successful. Further, a FISA amendment regarding physical searches could facilitate access to tax and other records that now, by statute, may be acquired only with a warrant based upon a full criminal standard.[190] The prospect of extending FISA to physical searches has been under consideration since before FISA became law[191] and there continue to be periodic indications of interest on the part of the Congress in such legislation.[192] While development and negotiation of a statutory framework for intelligence-related physical searches could be a challenging and grueling process, it would appear from the successful implementation of FISA that the benefits of public assurance and clear governmental authority would be well worth the effort.

---

[189] *See supra* notes 93-94, 125 and accompanying text. Similar arguments can also be expected to be raised, with added vigor, with regard to another potential area for FISA coverage that was put off originally by Congress but will likely grow in importance as technological change heightens the need for statutory authority; interception of international communications of United persons who are in the United States. *See* H.R. REP. No. 1293, Pt. I, 95th Cong., 2d Sess. 27-28, 50-51 (1978).

[190] *See, e.g.*, 26 U.S.C. § 6103(i) (1982) (tax return information); 39 U.S.C. § 3623(d) (opening of mail).

[191] In the late 1970s, an effort to develop a comprehensive oversight charter for the entire intelligence community included the provisions that ultimately became FISA but also would have provided the FISC with authority to approve physical searches for national security purposes. *See Hearings Before the Select Committee on Intelligence of the United States Senate on S. 2525, the National Intelligence Reorganization and Reform Act of 1978*, 95th Cong., 2d Sess. 973-1016 (1978). *See also* J. OSETH, REGULATING U.S. INTELLIGENCE OPERATIONS: A STUDY IN DEFINITION OF THE NATIONAL INTEREST 107-112, 122-48 (1985). Ultimately, the only portion of this enormous legislative effort that was enacted related solely to legislative oversight of intelligence activities. 50 U.S.C. § 413 (1982). *See* J.OSETH, *supra*, at 133-48; A.B.A. Standing Committee on Law and National Security, Oversight and Accountability of the U.S. Intelligence Agencies: An Evaluation 11 (1985).

[192] *See, e.g.*, SENATE SELECT COMM. ON INTELLIGENCE OF THE UNITED STATES SENATE, MEETING THE ESPIONAGE CHALLENGE: A REVIEW OF UNITED STATES COUNTERINTELLIGENCE AND SECURITY PROGRAMS, S. REP. No. 522, 99th Cong., 2d Sess. 54, 56 (1986); SSCI FISA REP. 660, *supra* note 117, at 17-20; SSCI FISA REP. 691, *supra* note 121, at 5-6.

CONCLUSION

It may be said with assurance that FISA has proven over its ten-year lifetime to have been a very successful experiment in national security legislation. As William Webster, then FBI Director, now Director of Central Intelligence, testified shortly after FISA was enacted, "We have had occasion to test most aspects of the statute and have found them to permit necessary intelligence collection. We are convinced that it provided our personnel with the assurance that their activities today will withstand challenge in the future."[193]

The Executive has obtained over four thousand surveillance orders from the FISC, allowing it to pursue activities it believed served the national security interests of the United States. Neither Congress nor the courts have found any basis for concluding that these surveillances have involved abuse of the statute, thus giving the public substantial assurance that individual rights are not being trammeled in pursuit of national security. The government agents and the private sector personnel who are involved in the conduct of these surveillances are able to rely upon judicial approval, thus protecting themselves from civil or criminal liability in performing their duties. These benefits support amending FISA so that it remains effective during the next ten years in the face of change and so a broader range of intelligence operations, including intelligence-related physical searches, can be brought under its authority.

[193] SSCI FISA REP. 660, *supra* note 117, at 4.