The System of Foreign Intelligence Surveillance Law

Peter P. Swire*

* Professor, Moritz College of Law of the Ohio State University and John Glenn Scholar in Public Policy Research. I thank the people with experience in foreign intelligence law who helped me in this project, many of whom prefer not to be identified. Stewart Baker, Jerry Berman, Jim Dempsey, John Podesta, and Ruth Wedgwood are among those who have helped teach me this topic. I am grateful for comments on earlier drafts from Susan Freiwalld, Beryl Howell, Kim Lane Scheppelle, Peter Raven-Hansen, Coleen Rowley, Stephen Saltzbugn, Michael Vatis, and those who attended my presentations at the Association of American Law Schools annual conference, The George Washington University Law School, the Moritz College of Law, and the University of Toledo School of Law. My thanks to Najah Allen, Katy Delaney, Heather Hostetler, and Scott Zimmerman for research assistance, and to the Moritz College of Law and the John Glenn Institute for research support.
I. National Security Surveillance Before 1978

The legal standard for "national security" or "foreign intelligence" surveillance results from the interaction of two conflicting positions. The first position is that wiretaps taking place on American soil should be treated like wiretaps used for law enforcement purposes, with the same Fourth Amendment protections. The second position is that the President has special authority over national security issues, and therefore can authorize wiretaps with fewer or no Fourth Amendment limits. This Part of the Article examines the legal basis for the two positions and then examines the sobering history of problems arising from domestic surveillance before 1978.
B. The Law and Logic of National Security Wiretaps

This history of applying the Fourth Amendment and the rule of law to wiretaps is accompanied by a second history, that of using wiretaps and other surveillance tools to protect the national security. Consider the Cold War example of an employee of the Soviet Embassy. What should the standards have been for wiretaps of that employee, who might also be an agent of the KGB? A Title III wiretap would often be impossible to get, because there would be no probable cause that a crime had been or would be committed. Yet this potential or known spy plausibly posed a serious threat to national
security. A wiretap might create extremely useful intelligence about the Soviet agent’s confederates and actions.

For many people, including those generally inclined to support civil liberties, the example of a known spy operating within the United States provides an especially compelling case for allowing wiretaps and other surveillance. Spies operating within the United States pose a direct threat to national security. For instance, spies can and have turned over nuclear and other vital military secrets to foreign powers. At the same time, some of the usual safeguards on wiretaps seem inappropriate when applied to foreign agents. Notifying the target of a criminal wiretap after the fact is required by the notice component of the Fourth Amendment and can be a crucial safeguard because it alerts citizens and the press of any overuse or abuse of the wiretap power. By contrast, notifying a foreign agent about a national security power can compromise sources and methods and create a diplomatic scandal. Similarly, minimization in the domestic context helps preserve the privacy of individuals who are not the target of a criminal investigation. Minimization in the foreign intelligence context, by contrast, can mean discarding the only hints available about the nature of a shadowy and hard-to-detect threat to security.

During wartime especially, it is easy to see how the temptation to use “national security” wiretaps against spies and foreign enemies, even on U.S. soil, would be irresistible. The legal basis for such a national security power can be derived from the text of the Constitution. The President is named Commander in Chief of the armed forces, and domestic actions against foreign powers may be linked to military and intelligence efforts abroad. This explicit grant of power to the President is supplemented by vague and potentially very broad language in Article II of the Constitution, that the President shall exercise the “executive power” and “take Care that the Laws be faithfully executed.” Going beyond the text, the Supreme Court in 1936, in United States v. Curtiss-Wright Export Corp., relied on the structure of the Constitution and the nature of sovereign nations to establish the “plenary and exclusive power of the President as the sole organ of the federal government in the field of international relations.”

President Franklin Roosevelt, responding to the Second World War, was the first President to authorize wiretaps on national security grounds. The use of such wiretaps expanded during the Cold War. In 1967, in Katz, the Supreme Court declined to extend its holding to cases “involving the national

33 U.S. CONST. art. II, § 3.
35 Id. at 320.
36 See Alison A. Bradley, Comment, Extremism in the Defense of Liberty?: The Foreign Intelligence Surveillance Act and the Significance of the USA PATRIOT ACT, 77 TUL. L. REV. 465, 468 (2002) (describing limited nature of national security wiretaps authorized by President Roosevelt).
security." In 1971, Justice Stewart summarized the expansion of the executive power that "in the two related fields of national defense and international relations[,] . . . largely unchecked by the Legislative and Judicial branches, has been pressed to the very hilt since the advent of the nuclear missile age."

The Supreme Court finally addressed the lawfulness of national security wiretaps in 1972 in United States v. United States District Court, generally known as the "Keith" case after the name of the district court judge in the case. The defendant, Plamondon, was charged with the dynamite bombing of an office of the Central Intelligence Agency in Michigan. During pretrial proceedings, the defendants moved to compel the United States to disclose electronic surveillance information that had been obtained without a warrant. The Attorney General submitted an affidavit stating that he had expressly approved the wiretaps, which were used "to protect the nation from attempts of domestic organizations to attack and subvert the existing structure of the Government." The United States objected to disclosure of the surveillance materials, claiming that the surveillance was a reasonable exercise of the President's power (exercised through the Attorney General) to protect the national security. Both the district court and the circuit court held for the defendant.

The Supreme Court unanimously affirmed. Justice Powell's opinion found that Title III, by its terms, did not apply to the protection of "national security information" and that the statute did not limit "the constitutional power of the President to take such measures as he deems necessary to protect the United States against the overthrow of the Government by force or other unlawful means." As it turned to the constitutional discussion of the scope of the Fourth Amendment, the Court expressly reserved the issues of foreign intelligence surveillance that are now covered by FISA: "[T]he instant case requires no judgment on the scope of the President's surveillance power with respect to the activities of foreign powers, within or without this country."

The Court then turned to the question left open by Katz: "Whether safeguards other than prior authorization by a magistrate would satisfy the

40 Id.
41 Id. at 299.
42 Id. at 299–300.
43 Id. at 300 n.2.
44 See id. at 301.
45 Id.
46 Id. at 324 (noting that "Mr. Justice Rehnquist took no part in the consideration or decision of this case").
47 Id. at 302 (quoting 18 U.S.C. § 2511(3)).
48 Id. at 308. Later, the Court reiterated the point: "We have not addressed, and express no opinion as to, the issues which may be involved with respect to activities of foreign powers or their agents." Id. at 321–22 (citation omitted).
Fourth Amendment in a situation involving the national security.'”49 The Government sought an exception to the Fourth Amendment warrant requirement, relying on the inherent presidential power and duty to “‘preserve, protect, and defend the Constitution of the United States.’”50 The Court acknowledged the importance of that duty, yet held that a warrant issued by a neutral magistrate was required for domestic security wiretaps.51 Noting the First Amendment implications of excessive surveillance, the Court concluded: “Security surveillances are especially sensitive because of the inherent vagueness of the domestic security concept, the necessarily broad and continuing nature of intelligence gathering, and the temptation to utilize such surveillances to oversee political dissent.”52

While recognizing the potential for abuse in domestic security wiretaps, the Court also recognized the “different policy and practical considerations from the surveillance of ‘ordinary crime.’”53 The list of possible differences is entirely familiar to those engaged in the debates since September 11: the gathering of security intelligence is often for a long term; it involves “the interrelation of various sources and types of information”; the “exact targets of such surveillance may be more difficult to identify”; and there is an emphasis on “the prevention of unlawful activity.”54 In light of these differences, the nature of “reasonableness” under the Fourth Amendment can shift somewhat. The Court invited legislation: “Congress may wish to consider protective standards for . . . [domestic security] which differ from those already prescribed for specified crimes in Title III.”55 The Court specifically suggested creating a different standard for probable cause and designating a special court to hear the wiretap applications,56 two invitations taken up by Congress in FISA.

C. National Security Wiretaps and “The Lawless State”

The Supreme Court’s invitation was eventually accepted by Congress in 1978 in FISA.57 FISA was enacted at a unique time, in the wake of Watergate and spectacular revelations about illegal actions by U.S. intelligence agencies. In my opinion, anyone who wishes to debate FISA and possible amendments to it has a responsibility to consider the history of this period. I am not a pessimist who believes that intelligence activities inevitably will return to the level of lawlessness at that time. I do believe, however, that human nature has remained largely unchanged since then. Unless effective institutional safeguards exist, large and sustained expansions of domestic in-

49 Id. at 309 (quoting Katz v. United States, 389 U.S. 347, 358 n.23).
50 Id. at 310 (quoting U.S. CONST. art. II, § 1).
51 Id. at 319–21.
52 Id. at 320.
53 Id. at 322.
54 Id.
55 Id.
56 Id. at 323.
intelligence activity, in the name of national security, can quite possibly re-create the troublesome behaviors of the past.

One particularly detailed account of the earlier period is a 1977 book by Morton Halperin, Jerry Berman and others entitled *The Lawless State: The Crimes of the U.S. Intelligence Agencies.* That book devotes an annotated chapter to the illegal surveillance activities of several U.S. agencies—the FBI, the CIA, the Army, the IRS, and others. The most famous discussion of the deeds and misdeeds of the intelligence agencies are the reports by the Senate Select Committee to Study Government Operations with Respect to Intelligence Activities, known as the “Church Committee” after its chairman, Frank Church. The 1976 final report summarized the number of people affected by domestic intelligence activity:

FBI headquarters alone has developed over 500,000 domestic intelligence files, and these have been augmented by additional files at FBI Field Offices. The FBI opened 65,000 of these domestic intelligence files in 1972 alone. In fact, substantially more individuals and groups are subject to intelligence scrutiny than the number of files would appear to indicate, since typically, each domestic intelligence file contains information on more than one individual or group, and this information is readily retrievable through the FBI General Name Index.

The number of Americans and domestic groups caught in the domestic intelligence net is further illustrated by the following statistics:

— Nearly a quarter of a million first class letters were opened and photographed in the United States by the CIA between 1953–1973, producing a CIA computerized index of nearly one and one-half million names.

— At least 130,000 first class letters were opened and photographed by the FBI between 1940–1966 in eight U.S. cities.

— Some 300,000 individuals were indexed in a CIA computer system and separate files were created on approximately 7,200 Americans and over 100 domestic groups during the course of CIA’s Operation CHAOS (1967–1973).

— Millions of private telegrams sent from, to, or through the United States were obtained by the National Security Agency from 1947 to 1975 under a secret arrangement with three United States telegraph companies.

— An estimated 100,000 Americans were the subjects of United States Army intelligence files created between the mid 1960s and 1971.

---


— Intelligence files on more than 11,000 individuals and groups were created by the Internal Revenue Service between 1969 and 1973 and tax investigations were started on the basis of political rather than tax criteria.

— At least 26,000 individuals were at one point catalogued on an FBI list of persons to be rounded up in the event of a “national emergency.”

These statistics give a flavor for the scale of domestic surveillance. Rather than repeat the history in detail here, it is helpful to identify themes that show the important concerns raised by improper surveillance. These are discussed below.

1. **Routine Violations of Law**

In *The Lawless State* the authors identify and document literally hundreds of separate instances of criminal violations by intelligence agencies. The Church Committee reported “frequent testimony that the law, and the Constitution were simply ignored.” The Committee quoted testimony from the man who headed the FBI’s Intelligence Division for ten years: “[N]ever once did I hear anybody, including myself, raise the question: ‘Is this course of action which we have agreed upon lawful, is it legal, is it ethical or moral.’ We never gave any thought to this line of reasoning, because we were just naturally pragmatic.” Instead of concern for the law, the intelligence focus was on managing the “flap Potential”—the likely problems if their activities became known.

2. **Expansion of Surveillance for Prevention and Other Purposes**

After World War II, “preventive intelligence about ‘potential’ espionage or sabotage involved investigations based on political affiliations and group membership and association. The relationship to law enforcement was often remote and speculative . . . .” Until the Church Committee’s hearings, the FBI continued to collect domestic intelligence under “sweeping authorizations” for investigations of “subversives, potential civil disturbances, and ‘potential crimes.’” Based on its study of the history, the Church Committee concluded:

The tendency of intelligence activities to expand beyond their initial scope is a theme which runs through every aspect of our investigative findings. Intelligence collection programs naturally generate

---

60 *Id.* (footnotes omitted).
61 *E.g., Halperin et al., supra note 58, at 3 (estimating the number of surveillance crimes committed); id. at 93 (describing surveillance violations by the FBI)).
63 *Id.*
64 *Id.*
66 *Id.*
ever-increasing demands for new data. And once intelligence has been collected, there are strong pressures to use it against the target.67

3. Secrecy

An essential aspect of domestic intelligence was secrecy:

Intelligence activity . . . is generally covert. It is concealed from its victims and is seldom described in statutes or explicit executive orders. The victim may never suspect that his misfortunes are the intended result of activities undertaken by his government, and accordingly may have no opportunity to challenge the actions taken against him.68

It was only in the wake of the extraordinary events of Watergate and the resignation of President Richard Nixon that Congress and the public had any inkling of the scope of domestic intelligence activities. That realization of the scope led directly to thoroughgoing legal reforms (many of which are being rolled back or questioned in the wake of September 11).

4. Use Against Political Opponents

The Church Committee documented that: “Each administration from Franklin D. Roosevelt’s to Richard Nixon’s permitted, and sometimes encouraged, government agencies to handle essentially political intelligence.”69 Wiretaps and other surveillance methods were used on members of Congress, Supreme Court Justices, and numerous mainstream and nonmainstream political figures. The level of political surveillance and intervention grew over time.70 By 1972, tax investigations at the IRS were targeted at protesters against the Vietnam War,71 and “the political left and a large part of the Democratic party [were] under surveillance.”72

5. Targeting and Disruption of Unpopular Groups, Including the Civil Rights Movement

The FBI’s COINTELPRO—counterintelligence program—“was designed to ‘disrupt’ groups and ‘neutralize’ individuals deemed to be threats to national security.”73 Targets for infiltration included the Ku Klux Klan and the Black Panthers. A special target was Martin Luther King, Jr., from late 1963 until his death in 1968. The Church Committee report explained:

---

67 Church Final Rep. IIa, supra note 59.
68 Id.
69 Id.
70 “The FBI practice of supplying political information to the White House . . . under the administrations of President Lyndon Johnson and Richard Nixon . . . grew to unprecedented dimensions.” Church Final Rep. IIb, supra note 65.
71 Id. Examining evidence of use of intelligence information against political opponents, the committee concluded: “A domestic intelligence program without clearly defined boundaries almost invited such action.” Id.
72 Halperin et al., supra note 58, at 124.
73 Church Final Rep. IIa, supra note 59.
In the words of the man in charge of the FBI’s “war” against Dr. King, “No holds were barred. . . . The program to destroy Dr. King as the leader of the civil rights movement included efforts to discredit him with executive branch officials, Congressional leaders, foreign heads of state, American ambassadors, churches, universities, and the press.”

In one especially ugly episode, Dr. King was preparing to go to Sweden to receive the Nobel Peace Prize when the FBI sent him an anonymous letter threatening to release an embarrassing tape recording unless he committed suicide.

6. Chilling of First Amendment Rights

The FBI’s COINTELPRO program targeted “speakers, teachers, writers, and publications themselves.” One internal FBI memorandum “called for ‘more interviews’ with New Left subjects ‘to enhance the paranoia endemic in these circles’ and ‘get the point across there is an FBI agent behind every mailbox.’” Once a federal agency is trying to get the message out that there is an “agent behind every mailbox,” then the chilling effect on First Amendment speech can be very great indeed.

7. Harm to Individuals

The hearings in the 1970s produced documented cases of harm to individuals from intelligence actions. For instance, an anonymous letter to an activist’s husband accused his wife of infidelity and contributed strongly to the breakup of the marriage. Also, “a draft counsellor deliberately, and falsely, accused of being an FBI informant was ‘ostracized’ by his friends and associates.” In addition to “numerous examples of the impact of intelligence operations,” the Church Committee concluded that “the most basic harm was to the values of privacy and freedom which our Constitution seeks to protect and which intelligence activity infringed on a broad scale.”

8. Distortion of Data to Influence Government Policy and Public Perceptions

Used properly, intelligence information can provide the President and other decisionmakers with the most accurate information possible about risks to national security. The Church Committee found that intelligence agencies sometimes warped intelligence to meet their political goals:

---

74 Id.
75 See HALPERIN ET AL., supra note 58, at 86. The Church Committee reported on the breadth of the FBI’s infiltration of the black community: “In 1970, the FBI used its ‘established informants’ to determine the ‘background, aims and purposes, leaders and Key Activists’ in every black student group in the country, ‘regardless of [the group’s] past or present involvement in disorders.’” CHURCH FINAL REP. IIb, supra note 65.
76 CHURCH FINAL REP. IIa, supra note 59.
77 Id.
78 Id.
79 Id.
80 Id.
The FBI significantly impaired the democratic decisionmaking process by its distorted intelligence reporting on communist infiltration of and influence on domestic political activity. In private remarks to Presidents and in public statements, the Bureau seriously exaggerated the extent of communist influence in both the civil rights and anti-Vietnam war movements.81

9. Cost and Ineffectiveness

The Church Committee concluded: “Domestic intelligence is expensive . . . . Apart from the excesses described above, the usefulness of many domestic intelligence activities in serving the legitimate goal of protecting society has been questionable.”82 After reviewing the effectiveness of various aspects of domestic intelligence, the Committee’s chief recommendation was “to limit the FBI to investigating conduct rather than ideas or associations.”83 The Committee also specifically recommended continued “intelligence investigations of hostile foreign intelligence activity.”84

In summary, the history shows numerous concrete examples of law-breaking by the U.S. intelligence agencies. More generally, the history helps show how secret information gathering and disruption of political opponents over time can threaten democracy itself. The fear is that leaders using “dirty tricks” and secret surveillance can short-circuit the democratic process and entrench themselves in power. The legal question is how to construct checks and balances that facilitate needed acts by the government but which also create long-term checks against abuse.

II. The 1978 Compromise: The Foreign Intelligence Surveillance Act

At the level of legal doctrine, FISA was born from the two legal traditions discussed in Part I: the evolving Supreme Court jurisprudence that wiretaps required judicial supervision, and the continuing national security imperative that at least some foreign intelligence wiretaps be authorized. At the level of practical politics, FISA arose from the debate between the intelligence agencies, who sought maximum flexibility to protect national security, and the civil libertarians, who argued that the abuses revealed by the Church Committee should be controlled by new laws and institutions.85

The clear focus of FISA, as shown by its title, was on foreign rather than domestic intelligence. The statute authorized wiretaps and other electronic surveillance against “foreign powers.”86 These “foreign powers” certainly included the communist states arrayed against the United States in the Cold War. The definition was broader, however, including any “foreign govern-

82 CHURCH FINAL REP. IIa, supra note 59.
83 Id.
84 Id.
85 Hearing on Foreign Intelligence Surveillance Act, 95th Cong. 147–48 (1979) (statement of Jerry Berman).
86 The current definition is codified at 50 U.S.C. § 1801(a) (2000).
ment or any component thereof, whether or not recognized by the United States."87 A “foreign power” included a “faction of a foreign nation,” or a foreign-based political organization, not substantially composed of United States persons.”88 Even in 1978, the definition also included “a group engaged in international terrorism or activities in preparation therefor.”89

Surveillance could be done against an “agent of a foreign power,” which classically would include the KGB agent or someone else working for a foreign intelligence service.90 An “agent of a foreign power” could also include a person who “knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power.”91 The definition of “international terrorism” had three elements: violent actions in violation of criminal laws; an intent to influence a government by intimidation or coercion; and actions that transcend national boundaries in their method or aims.92

The Act drew distinctions between U.S. persons and non-U.S. persons.93 The former consists essentially of U.S. citizens and permanent residents.94 Non-U.S. persons could qualify as an “agent of a foreign power” simply by being an officer or employee of a foreign power, or a member of an international terrorist group.95 The standards for surveillance against U.S. persons were stricter, in line with the Church Committee concerns about excessive surveillance against domestic persons. U.S. persons qualified as an “agent of a foreign power” only if they knowingly engaged in listed activities, such as clandestine intelligence activities for a foreign power, which “involve or may involve a violation of the criminal statutes of the United States.”96

In FISA, Congress accepted in large measure the invitation in Keith to create a new judicial mechanism for overseeing national security surveillance.97 The new statute used the terms “foreign power” and “agent of a foreign power” employed by the Supreme Court in Keith, where the Court specifically said that its holding applied to domestic security wiretaps rather

---

88 Id. § 1801(a)(2), (5).
89 Id. § 1801(a)(4).
90 See id. § 1801(b).
91 Id. § 1801(b)(2)(C).
92 See id. § 1801(c). The term “international terrorism” was defined in full as: [A]ctivities that—(1) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or any State; (2) appear to be intended—(A) to intimidate or coerce a civilian population; (B) to influence the policy of a government by intimidation or coercion; or (C) to affect the conduct of a government by assassination or kidnapping; and (3) occur totally outside the United States or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.

Id.
93 Id. § 1801(j).
94 Id.
95 Id. § 1801(b)(1)(A).
96 Id. § 1801(b)(2)(A).
than surveillance of "foreign powers." Instead of creating a special regime for domestic security, however, Congress decided to split surveillance into only two parts—the procedures of Title III, which would apply to ordinary crimes and domestic security wiretaps, and the special procedures of FISA, which would apply only to "agents of a foreign power."

A curious hybrid emerged in FISA between the polar positions of full Title III protections, favored by civil libertarians, and unfettered discretion of the executive to authorize national security surveillance, favored by the intelligence agencies. The statute required the Chief Justice to designate seven (now eleven) district court judges to the new Foreign Intelligence Surveillance Court ("FISC"). These judges had jurisdiction to issue orders approving electronic surveillance upon finding a number of factors, notably that "there is probable cause to believe that the target of the electronic surveillance is a foreign power or an agent of a foreign power." This probable cause standard looks to quite different facts than the Title III standard, which requires "probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense" for wiretaps to be permitted.

FISA orders contain some, but not all, of the other safeguards in Title III. Both regimes require high-level approval within the Department of Justice, with the Attorney General having to give personal approval for FISA applications. Both regimes require minimization procedures to reduce the effects on persons other than the targets of surveillance. Both provide for electronic surveillance for a limited time, with the opportunity to extend the surveillance. Both require details concerning the targets of the surveillance and the nature and location of the facilities placed under surveillance. Both allow "emergency" orders, where the surveillance can begin without judicial approval subject to quick, subsequent approval by a judge.

---

98 "Id. at 308, 321–22.
99 The 1978 law created the split by providing, in terms still effective today, that Title III and FISA "shall be the exclusive means by which electronic surveillance . . . and the interception of domestic wire and oral communications may be conducted." 18 U.S.C. § 2511(2)(f) (2000).
100 50 U.S.C. § 1803.
101 Id. § 1805(a)(3)(A).
As for differences, Title III gives discretion to the judge to refuse to issue the order, even where the statutory requirements have been met.108 Under FISA, however, the judge "shall" issue the order once the statutory findings are met.109 FISA has looser standards about whether other, less-intrusive surveillance techniques must first be exhausted.110

The most important difference is that the existence of a Title III wiretap is disclosed to the subject of surveillance after the fact, in line with the Fourth Amendment requirement that there be notice of government searches.111 By sharp contrast, the FISA process is cloaked in secrecy. Targets of FISA surveillance almost never learn that they have been subject to a wiretap or other observation. The only statutory exception is where evidence from FISA surveillance is used against an individual in a trial or other proceeding. In such instances, the criminal defendant or other person can move to suppress the evidence on the grounds that the information was unlawfully acquired or the surveillance did not comply with the applicable order. Even in this setting the individuals have no right to see the evidence against them. The judge, upon a motion by the Attorney General, reviews the evidence in camera (in the judge’s chambers) and ex parte (without assistance of defense counsel).112

The secrecy and ex parte nature of FISA applications are a natural outgrowth of the statute’s purpose, to conduct effective intelligence operations against agents of foreign powers.113 In the shadowy world of espionage and counterespionage, nations that are friends in some respects may be acting contrary to U.S. interests in other respects. Prudent foreign policy may suggest keeping tabs on foreign agents who are in the United States, but detailed disclosure of the nature of that surveillance could create embarrassing incidents or jeopardize international alliances.

Along with the limited nature of judicial supervision, Congress decided to create additional institutional checks on the issuance of the secret FISA

108 "Upon such application the judge may enter an ex parte order, as requested or as modified, authorizing or approving interception . . . ." 18 U.S.C. § 2518(3) (emphasis added).
110 Title III requires that a wiretap or other electronic surveillance be a last resort, available only when "normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous." 18 U.S.C. § 2518(3)(C). Under FISA, the application must simply certify "that such information cannot reasonably be obtained by normal investigative techniques." 50 U.S.C. § 1804(7)(C).
111 Title III requires notice "[w]ithin a reasonable time but not later than ninety days" after surveillance expires. 18 U.S.C. § 2518(8)(d). Notice is given to the persons named in the order and others at the judge's discretion. Id. An inventory is provided concerning the dates and scope of surveillance. Id. In the judge's discretion, the person or counsel may inspect such intercepted communications, applications, and orders as the judge determines to be in the interest of justice. Id. The judge may also, on a showing of good cause, postpone notice. Id.
112 These procedures are set forth in 50 U.S.C. § 1806. In ruling on a suppression motion, the judge "may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance." Id. § 1806(f). If the court determines that the surveillance was conducted lawfully, "it shall deny the motion of the aggrieved person except to the extent that due process requires discovery or disclosure." Id. § 1806(g).
wiretaps. To regularize congressional oversight, the Attorney General must report to the House and Senate Intelligence Committees every six months about FISA electronic surveillance, including a description of each criminal case in which FISA information has been used for law enforcement purposes.\footnote{See id. § 1808(a). In the initial years after passage of FISA, the Intelligence Committees were additionally required to report to the full House and Senate about the operation of the statute. Id. § 1808(b).} The Attorney General also must make an annual report to Congress and the public about the total number of applications made for orders and extensions of orders, as well as the total number that were granted, modified, or denied.\footnote{Id. § 1807.} This report is similar to that required for Title III wiretaps, but the latter provides additional details such as the types of crimes for which a wiretap is used and the number of wiretaps that resulted in successful prosecutions.\footnote{See 18 U.S.C. § 2529 (reports on Title III wiretaps); see also 18 U.S.C. § 3126 (2000) (reports on pen register and trap and trace orders).} Although the FISC ruled against an order for the first time in 2002, as described below,\footnote{See infra Part IV.C.} the annual FISA reports provide a rough guide of the extent of FISA surveillance.\footnote{See Electronic Privacy Information Center, Foreign Intelligence Surveillance Act Orders 1979–2002, http://www.epic.org/privacy/wiretap/stats/fisa_stats.html (last updated May 6, 2004) (giving annual statistics of FISA orders). The 2003 FISA Report stated that three additional orders were denied in 2003. Letter from William E. Moschella, U.S. Department of Justice, Office of Legislative Affairs, to L. Ralph Mecham, Director, Administrative Office of the United States Courts (Apr. 30, 2004), at http://www.epic.org/privacy/terrorism/fisa/2003_report.pdf. At the time of this writing, no further information was available to the public about the three denials.} Congress also relied on institutional structures within the executive branch to check overuse of domestic surveillance.\footnote{E.g., Jim McGee & Brian Duffy, Main Justice 309 (1996).} The requirement that the Attorney General authorize applications meant that the FBI on its own could no longer implement national security wiretaps. Applications by the FBI would need to be approved by the Justice Department. In light of the historical evidence about the independence of longtime FBI Director J. Edgar Hoover from control by the Justice Department,\footnote{See, e.g., Jeff Nesmith et al., Subtle Forces Swirl Just Beneath Siege Inquires: The tug of Personality Conflict in Washington Alters Flow of Waco Controversy, Austin Am. Statesman, Sept. 19, 1999, at A1 (discussing “tension” between the Department of Justice and the FBI, and between Attorney General Reno and FBI Director Freeh).} and the disagreements that have often continued between the FBI and the Department,\footnote{50 U.S.C. § 1805(a)(2).} this supervision by the Justice Department was a potentially significant innovation in FISA. Reacting to the historical evidence about surveillance of political speech and association, the 1978 statute provided that “no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States.”\footnote{50 U.S.C. § 1805(a)(3)(A).} This language reflects a congressional concern about infringement on First Amendment activities, but provides only modest safe-
guards, because an individual could apparently be considered an agent of a foreign power based "largely" or "substantially" on protected activities.

Finally, the text of the 1978 statute showed that the purpose of the FISA wiretaps was foreign intelligence rather than preventing or prosecuting crimes. The Church Committee and other revelations of the 1970s had shown that the FBI had used the risk of "subversion" and other potential crimes as the justification for investigating a vast array of political and other domestic activity. The 1978 statute therefore specified that the application for a FISA order certify that "the purpose of the surveillance is to obtain foreign intelligence information."124

In summary, the 1978 FISA revealed a grand compromise between the advocates for civil liberties and the intelligence community. From the civil liberties side, FISA had the advantage of creating a legal structure for foreign intelligence surveillance that involved Article III judges. It had the disadvantage of having standards that were less protective overall than were constitutionally and statutorily required for investigations of domestic crimes. In particular, the notice requirement of the Fourth Amendment did not apply, and targets of FISA surveillance usually never learned they were the objects of government searches. From the intelligence perspective, FISA had the disadvantage of imposing bureaucratic rules and procedures on searches that had previously been done subject to the inherent authority of the President or the Attorney General. An advantage, which became more evident over time, was that FISA provided legislative legitimation for secret wiretaps, and created standardized bureaucratic procedures for getting them. By establishing these clear procedures, it became easier over time for the number of FISA surveillance orders to grow. To describe the compromise in another way, FISA set limits on surveillance by "The Lawless State," but gave "The Lawful State" clear rules that permitted surveillance.

III. FISA from 1978 to 2001

FISA was part of a broad-based effort in the wake of Watergate to place limits on the Imperial Presidency and its surveillance activities. The Privacy Act of 1974 clamped down on secret files on Americans and created new legal rules for how personal information could be used by federal agencies. The Freedom of Information Act was broadened substantially in 1974, and greater openness in government was encouraged by the Govern-

123 See Church Final Rep. II, supra note 59 (noting that between 1960 and 1974, "subversion" alone was used to justify more than 500,000 investigations, with apparently no prosecutions for the actual crimes).


ment in the Sunshine Act,128 new rules in legislatures to open up committee hearings to the public,129 and more aggressive investigative journalism in the wake of the revelations by Bob Woodward and Carl Bernstein.130

The FBI in particular had to change its operations, including its domestic surveillance activities, in the wake of the revelations about "The Lawless State." The best-known limits on the FBI's activities were the Guidelines on Domestic Surveillance issued by Attorney General Edward Levi in 1976 ("Levi Guidelines").131 The guidelines limited domestic security investigations to activities that both "involve or will involve the use of force or violence" and "involve or will involve the violation of federal law."132 The Levi Guidelines defined procedures and time limits for preliminary, limited, and full investigations. The FBI was required to report in detail about investigations to the Department of Justice, and the Attorney General or his designees had the power to terminate investigations at any time. To address concerns about intrusion into First Amendment activity, the Guidelines stated that all domestic security investigations "shall be designed and conducted so as not to limit the full exercise of rights protected by the Constitution and laws of the United States."133

The Levi Guidelines represented a judgment that the best way to save the FBI as an effective agency was to demonstrate that it had come within the rule of law. Greater oversight of investigations by the Justice Department was central to the new approach: "If the FBI would play by the new rules, the Justice Department would defend it to the hilt."134 The FBI likely shifted over time to a much higher compliance with legal rules than had been true before the revelations of the 1970s.135

133 Id.
134 McGee & Duffy, supra note 120, at 311.
135 For instance, shortly after I left the government I had a lengthy conversation with a senior FBI lawyer who had watched the changes over previous decades. He frankly admitted that the Bureau had not worried much about breaking the law before the mid-1970s. He said that the painful revelations and the bad effects on the careers of those caught up in those revelations had led to a profound change in the organization's culture. The Bureau, by early 2001, had developed a culture of compliance. These statements tracked the views of a very knowledgeable insider with whom I worked in government. He agreed that the FBI had generally learned to follow the rules since the 1970s. He also believed that they often had very aggressive interpretations of the rules, and they stayed within the limits of their interpretation.

This shift to a culture of compliance has some important implications. First, these observa-
The implementation of FISA after 1978 followed a similar pattern of Justice Department oversight of the FBI. Mary Lawton, the lead drafter of the Levi Guidelines, eventually became the chief of the Office of Intelligence Policy and Review ("OIPR") within the Justice Department.\textsuperscript{136} Previously, the FBI had forum shopped in different parts of the Justice Department to get approval for domestic surveillance. Now the OIPR became the gatekeeper for all applications to the FISC. Mary Lawton, who had finished first in her class at the Georgetown Law Center, sat at the center of the process, applying "Mary's Law" to applications for FISA surveillance.\textsuperscript{137}

The 1996 book \textit{Main Justice}, which provides the most detailed public writing about the period, summarizes the combined effect of having FISA applications signed by the intelligence agent, the lawyer who drafted it, the head of the intelligence agency, and the Attorney General:

All those signatures served a purpose, to assure the federal judge sitting in the FISA court that a national security wiretap was being sought for "intelligence purposes" and for no other reason—not to discredit political enemies of the White House, not to obtain evidence for a criminal case through the back door of a FISA counterintelligence inquiry.\textsuperscript{138}

This is consistent with my view of perhaps the most controversial change in FISA in the Patriot Act—the breaking down of the "wall" between foreign intelligence and law enforcement activities. My own understanding is that the wall has existed since the creation of FISA in 1978, but there has always been a gate in it. The OIPR has been the gatekeeper. It has permitted foreign intelligence information to go to law enforcement in a limited number of cases, but it has historically remained mindful of the basic dictate of FISA, that the purpose of FISA surveillance was for foreign intelligence and that there should be safeguards on the domestic surveillance that had created such problems in the period of "The Lawless State."

This understanding is consistent with the text of FISA and the actions of the Justice Department in 1995. As discussed above, the text of the original FISA stated that "the purpose" of the surveillance was "to obtain foreign intelligence information."\textsuperscript{139} The text also provided mechanisms for using information from FISA wiretaps in court, subject to special rules about in camera review by the judge of the FISA material.\textsuperscript{140} Taken together, the text

\begin{footnotesize}
\textsuperscript{136} McGee & Duffy, supra note 120, at 314.
\textsuperscript{137} For an admiring portrait of Mary Lawton and her role in shaping foreign intelligence law until her death in 1993, see the chapter entitled "Mary's Law" in McGee & Duffy, supra note 120, at 303–19.
\textsuperscript{138} Id. at 318.
\textsuperscript{139} See supra note 124 and accompanying text.
\textsuperscript{140} Id.
\end{footnotesize}
suggests a preponderance of use of the special wiretaps for foreign intelligence, with use for law enforcement only where the evidence was developed in the course of a bona fide foreign intelligence surveillance.\textsuperscript{141} In 1995, two years after the death of Mary Lawton, Attorney General Janet Reno issued confidential guidelines to formalize procedures for contacts among the FBI, the Criminal Division, and OIPR for foreign intelligence and foreign counterintelligence investigations.\textsuperscript{142} The guidelines gave OIPR a central role in the process. Both the FBI and the Criminal Division, for instance, were required to notify OIPR of contacts with each other concerning such investigations, and contacts between the FBI and the Criminal Division were logged.\textsuperscript{143} The FBI was generally prohibited from contacting any U.S. Attorney's Office concerning such investigations without prior permission of both OIPR and the Criminal Division.\textsuperscript{144} OIPR was further directed to inform the FISC "of the existence of, and basis for, any contacts among the FBI, the Criminal Division, and a U.S. Attorney's Office, in order to keep the FISC informed of the criminal justice aspects of the ongoing investigation."\textsuperscript{145}

Alongside these developments in the Justice Department, FISA changed only modestly from 1978 until the events of September 11, 2001. Federal courts upheld FISA against constitutional challenges.\textsuperscript{146} The courts also upheld some broadening of the purpose requirement, allowing surveillance where "the primary purpose," rather than "the purpose," was to gather foreign intelligence information.\textsuperscript{147}

Although FISA originally applied only to electronic surveillance, Congress gradually widened its scope to other tools commonly used by law enforcement in criminal cases. After Attorney General Reno relied on her inherent powers to authorize physical surveillance of CIA spy Aldrich Ames's home, the Justice Department requested and received the authority in 1995 to apply to the FISC for physical searches.\textsuperscript{148} In 1998, the Act was extended to include pen register and trap and trace orders (listing of the tele-

\textsuperscript{141} The Senate Report on FISA stated, "'Contrary to the premises which underlie the provision of Title III of the Omnibus Crime Control Act of 1968 . . . it is contemplated that few electronic surveillances conducted pursuant to [FISA] will result in criminal prosecution.'" McGee & Duffy, supra note 120, at 326–27 (quoting members of the Senate Select Committee on Intelligence, 1978 Report).

\textsuperscript{142} Memorandum from Janet Reno, Attorney General, to Assistant Attorney General, Criminal Division, FBI Director, Counsel for Intelligence Policy, and United States Attorneys (July 19, 1995), http://www.fas.org/irp/agency/doj/fisa/1995procs.html. For a description of the genesis and contents of the 1995 guidelines, see McGee & Duffy, supra note 120, at 327–43.

\textsuperscript{143} Memorandum from Janet Reno, supra note 142.

\textsuperscript{144} Id. § A.2.

\textsuperscript{145} Id. § A.7.

\textsuperscript{146} E.g., United States v. Duggan, 743 F.2d 59, 71 (2d Cir. 1984) (no violation of Fourth Amendment or the separation of powers); United States v. Belfield, 692 F.2d 141, 149 (D.C. Cir. 1982) (no violation of Fifth or Sixth Amendment rights); United States v. Falvey, 540 F. Supp. 1306, 1313 (E.D.N.Y. 1982) (no violation of First Amendment rights).

\textsuperscript{147} Duggan, 743 F.2d at 77–78. For a discussion of other cases that also used the "primary purpose" test, see infra note 217 and accompanying text.

phone numbers and similar information contacted by an individual). The same year, the Act was extended to permit access to limited forms of business records, notably including vehicle rental records of the sort relevant to investigations of the Oklahoma City and first World Trade Center bombings. These extensions were analogous to FISA electronic surveillance, with the primary purpose to gather information on foreign powers or agents of foreign powers.

The most significant change was likely the increased number of FISA orders. Once the FISA system was up and running in 1981, there remained between 433 and 600 orders for each year through 1994, except for a one-year total of 635 in 1984. In 1995, 697 orders were granted, growing in subsequent years to 839, 748, 796, 880, and 1012 during President Clinton’s term. FISA orders fell to 934 in 2001, and grew to record numbers of 1228 in 2002 and 1727 in 2003. By comparison, the number of federal Title III wiretap orders in 1981 was 106, with a peak of 601 in 1999 and a total of 578 in 2003, the most recent year for which statistics are available. State law enforcement also conducted Title III wiretaps, with a total of 861 reported for 2002. Taken together, FISA wiretaps have grown substantially in the past decade, especially after September 11. Since the early 1980s they have constituted the majority of federal wiretaps.

In assessing the implementation of FISA from 1978 to early 2001, the basic structures from the 1970s remained fairly fixed. The bargain of FISA had been realized—the government could carry out secret surveillance in the United States, subject to limits to “foreign intelligence” activities and oversight by all three branches of government. The “wall” was in place, with the OIPR as the chief gatekeeper for exchange of information between the foreign intelligence and law enforcement operations. Despite the Levi Guidelines, there were some instances where civil liberties proponents produced evidence that “domestic surveillance” had interfered with First Amendment activities, but these instances seemed fairly few. There was some expansion of legal authority, but the greatest practical change was likely the increased number of FISA applications over time, especially since efforts to fight terrorism climbed during the 1990s.

---

150 Id. § 602, 112 Stat. at 2411–12 (codified at 50 U.S.C. §§ 1861–1862 (2000)) (permitting access held by common carriers, physical storage facilities, public accommodation facilities, and vehicle rental facilities).
151 Electronic Privacy Information Center, supra note 118.
152 Id.
153 Id.; Letter from William E. Moschella, supra note 118.
154 2003 WIRETAP REPORT, supra note 9, at 3.
155 Id. For discussion of the relative lack of institutional safeguards on wiretaps conducted at the state level, see Kennedy & Swire, supra note 20, at 977–83.
156 The greatest concerns were expressed about FBI surveillance of the Committee in Solidarity with the People of El Salvador in the 1980s. Attorney General’s Guidelines, supra note 131.
157 For instance, FISA wiretaps and search authorizations increased from 484 in 1992 to 839 in 1996 (after the Oklahoma City and first World Trade Center incidents), while federal Title III wiretaps increased more slowly, from 340 in 1992 to 581 in 1996. See Electronic Privacy Informa-