7
Wiretapping

Wiretapping is the traditional term for interception of telephone conversations. This should not be taken too literally. The word is no longer restricted to communications traveling by wire, and contemporary wiretaps are more commonly placed on radio links or inside telephone offices. The meaning has also broadened in that the thing being tapped need no longer be a telephone call in the classic sense; it may be some other form of electronic communication, such as fax or data.

Compared with the more precise but more general phrase "communications interception," the word "wiretapping" has two connotations. Much the stronger of these is that a wiretap is aimed at a particular target, in sharp contrast to the "vacuum cleaner" interception widely practiced by national intelligence agencies. The weaker connotation is that it is being done by the police.

The history of wiretapping in the United States is in fact two histories intertwined. It is a history of wiretapping *per se*—that is, a history of the installation and use of wiretaps by police, intelligence agencies, honest citizens, businesses, and criminals. It is also a history of society's legal response to wiretapping by these various groups.

The origins of wiretapping lie in two quite different practices: eavesdropping and letter opening. "Eavesdropping," although once more restricted in meaning,[1] has come to describe any attempt to overhear conversations without the knowledge of the participants. "Letter opening" takes in all acquisition, opening, reading, and copying of written messages, also without the knowledge of the sending and receiving parties. Telecommunication has unified and systematized these practices.

Before the electronic era, a conversation could only be carried on by people located within earshot of each other, typically a few feet apart. Neither advanced planning nor great effort on the part of the participants was required to ensure a high degree of security. Written communications were more vulnerable, but intercepting one was still a hit-or-miss affair. Messages traveled by a variety of postal services, couriers, travelers, and merchants. Politically sensitive messages, in particular, could not be counted on to go by predictable channels, so special couriers were sometimes employed.

And written messages enjoyed another sort of protection. Regardless of a spy's skill with flaps and seals, there was no guarantee that, if a letter was intercepted, opened, and read, the victim would not notice the intrusion. Since spying typically has to be done covertly in order to succeed, the chance of detection is a substantial deterrent.

Electronic communication has changed all this in three fundamental ways: it has made telecommunication too convenient to avoid; it has, despite appearances, reduced the diversity of channels by which written messages once traveled; and it has made the act of interception invisible to the target.

Conversation by telephone has achieved an almost equal footing with face-to-face conversation. It is impossible today to run a successful business without the telephone, and eccentric even to attempt to do without the telephone in private life. The telephone provides a means of communication so effective and convenient that even people who are aware of the danger of being overheard routinely put aside their caution and use it to convey sensitive information.

As the number of channels of communication has increased (there are now hundreds of communication companies, with myriad fibers, satellites, and microwave links), the diversity of communication paths has diminished. In the days of oxcart and sail, there was no registry of the thousands of people willing to carry a message in return for a tip from the recipient. Today, telecommunications carriers must be registered with national and local regulatory bodies and are well known to trade associations and industry watch groups. Thus, interception has become more systematic. Spies, no longer faced with a patchwork of *ad hoc* couriers, know better where to look for what they seek.

Perhaps more important, interception of telecommunications leaves no telltale "marks on the envelope." It is inherent in telecommunication—and inseparable from its virtues—that the sender and the receiver of a message have no way of telling who else may have recorded a copy.

Any discussion of wiretapping, particularly a legal discussion, is complicated by the fact that electronics has not only made interception of telecommunications possible; it has also made it easier to "bug" face-to-face conversations. Bugging would be nearly irrelevant to the central subject of this book—cryptography and secure telecommunications—were it not for the fact that bugs and wiretaps are inseparably intertwined in law and jurisprudence and named by one collective term: *electronic surveillance*.

Wiretaps and bugs are powerful investigative tools. They allow the eavesdropper to overhear conversations between politicians, criminals, lawyers, or lovers without the targets' knowing that their words are being shared with unwanted listeners. Electronic surveillance is a tool that can detect criminal conspiracies and provide prosecutors with strong evidence—the conspirators' incriminating statements in their own voices—all without danger to law-enforcement officers. On the other hand, the very invisibility on which electronic surveillance depends for its effectiveness makes it evasive of oversight and readily adaptable to malign uses.[2] Electronic surveillance can be and has been used by those in power to undermine the democratic process by spying on their political opponents. In light of this, it is not surprising that Congress and the courts have approached wiretapping and bugging with suspicion.

Today, communication enjoys a measure of protection under US law, and neither government agents nor private citizens are permitted to wiretap at will. This has not always been the case. The current view—that wiretaps are a kind of search—has evolved by fits and starts over a century and a half. The Supreme Court ruled in 1967 that the police may not employ wiretaps without court authorization. Congress has embraced this principle, limiting police use of wiretaps and setting standards for the granting of warrants. The same laws prohibit most wiretapping by private citizens.

The rules against unwarranted wiretapping are not absolute, however. For example, the courts ruled in 1992 (*United States v. David Lee Smith*,

978 F. 2nd 171, US App) that conversations over cordless phones were not protected and that police tapping of cordless phones did not require a search warrant. A 1994 statute (Communications Assistance for Law Enforcement Act of 1994, Public Law 103-414, §202) extended the warrant requirements of the earlier law to cover cordless phones. The law also makes some exceptions for businesses intercepting the communications of their own employees on company property.

Constitutional Protection

Protection for the privacy of communications stems primarily from the Fourth Amendment to the US Constitution. Epitomizing the underlying principle of the Bill of Rights—that individual citizens need protection against the power of the state—the Fourth Amendment asserts "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."

The Fourth Amendment was a response to the British writs of assistance, which empowered officers of the Crown to search "wherever they suspected uncustomed goods to be" and to "break open any receptacle or package falling under their suspecting eye" (Lassen 1937, p. 54). In framing the laws of the new nation, the founders sought to avoid creating such unrestricted governmental powers. However, they also recognized that since criminals try to hide the evidence of their crimes, law-enforcement officials must have the power to conduct searches. The Fourth Amendment thus allows searches, but restricts them, specifying that "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."

As written, the Fourth Amendment protects citizens against invasions of property. Although strongly suggested by the phrase "secure in their persons, houses, papers, and effects," the word 'privacy' is never used. The view that the Fourth Amendment protects things less tangible than property has taken more than a century to develop.

Wiretaps of the Nineteenth Century

When the telegraph joined the covered wagon and the stagecoach as a channel of long-distance communication, wiretapping followed quickly. During the Civil War, General Jeb Stuart traveled with his own tapper.[3] In California in 1864, a former stockbroker obtained market information by intercepting telegraph messages; he was prosecuted for violating a surprisingly early California statute against wiretapping (Dash et al. 1959, p. 23).

The convenience of voice communication made it obvious that intercepted telephone calls would be a rich source of information. In 1899 the *San Francisco Call* accused a rival, the *San Francisco Examiner*, of wiretapping conversations between the *Call* and its reporters and stealing the *Call*'s exclusives. In 1905, the California legislature responded by extending an 1862 law prohibiting telegraph wiretapping to telephones (ibid., pp. 25–26).

The first tapping of telephones by police occurred in the early 1890s in New York City. An 1892 New York State law had made telephone tapping a felony, but New York policemen believed that the law did not apply to them and employed wiretaps anyway (ibid., p. 35). In 1916 the mayor of New York was found to have authorized wiretapping of some Catholic priests in connection with a charity-fraud investigation, despite the fact that none of the priests were suspected of participating in the illegal activity (*New York Times* 1916). The state legislature discovered that the police had the ability to tap any line of the New York Telephone Company. Using this power with abandon, the police had listened in on confidential conversations between lawyers and their clients, and between physicians and their patients. The *New York Times* reported that "in some cases the trunk lines of hotels were tapped and the conversations of all hotel guests listened to" (ibid.).

During this period, the federal government played no legislative role—except during World War I, when concern that enemy agents would tap phone lines led to a federal Anti-Wiretap Statute (40 Stat. 1017, 1918). After the war, law-enforcement agencies began to find wiretapping increasingly valuable. Wiretapping is said to have been the most frequently used tool for catching bootleggers during Prohibition (Dash et al. 1959, p. 28).

The *Olmstead* Decision

As was mentioned in chapter 6, Roy Olmstead was caught running a $2 million-a-year bootlegging operation during Prohibition. Convicted partially on the basis of evidence obtained from warrantless wiretaps installed by federal agents, Olmstead appealed, and the case made its way to the US Supreme Court.

Though closely divided, the Court ruled that the evidence obtained by tapping the defendants' phone calls had not involved any trespass into their homes or offices. According to the Court: "There was no searching.... The evidence was secured by the use of ... hearing and that only...." (*Olmstead v. United States*, 277 US 438, 1928, p. 464) Five justices agreed that the Fourth Amendment protected tangibles alone, that conversation was an intangible, and that therefore using the evidence from the wiretaps did not constitute unreasonable search and seizure.

In his dissenting opinion in the *Olmstead* case (which has become one of the most quoted of judicial opinions), Justice Louis Brandeis argued that protections provided by the Bill of Rights should operate in a world of electronic communications. In 1928 the telephone was already necessary for commerce and was rapidly becoming an integral part of daily life. Brandeis described the threat that wiretapping posed to privacy:

> Whenever a telephone line is tapped, the privacy of the persons at both ends of the line is invaded, and all conversations between them upon any subject, and although proper, confidential and privileged, may be overheard. Moreover, the tapping of one man's telephone line involves the tapping of the telephone of every other person whom he may call, or who may call him. As a means of espionage, writs of assistance and general warrants are but puny instruments of tyranny and oppression when compared with wire-tapping. (Brandeis 1928, pp. 475–476)

Despite his eloquence, Brandeis's viewpoint did not carry the Court. There was widespread consternation over the Court's ruling, but although there were several attempts to do so, Congress did not make wiretapping illegal.

The *Nardone* Cases

In 1934, Congress passed the Federal Communications Act (FCA), which placed jurisdiction over radio and wire communications in the hands of the newly created Federal Communications Commission and established

a regulatory framework that has dominated American telecommunications ever since. The FCA prohibited the "interception and divulgence" of wire communications. Although its wording was quite similar to that of the Radio Act of 1927 (the law in effect at the time of the *Olmstead* case), the Supreme Court used the FCA to reverse *Olmstead*.

In *Olmstead*, the Court had ruled on constitutional grounds and had found warrantless wiretaps legal. A decade later, it considered the case of Frank Carmine Nardone, another accused bootlegger. This time, the Court ruled on the basis of the new law and held that information from wiretaps placed by federal agents was not admissible as evidence (*Nardone v. United States*, 302 US 379, 1937).

Two years later Nardone was back. Having been convicted in a new trial that used evidence derived from the warrantless wiretaps, Nardone appealed, arguing that the evidence should not be admissible. The Court concurred and held that information even indirectly derived from wiretaps could not be used as evidence (*Nardone v. United States*, 308 US 338, 1939). The same day, in a different case, the Supreme Court ruled that the FCA applied to federal wiretapping of intrastate as well as interstate communications (*Weiss v. United States*, 302 US 321, 1939). In response to these decisions, Attorney General Robert Jackson ordered a halt to FBI wiretapping (Gentry 1991, p. 231).

These decisions appeared to prohibit wiretapping by federal law-enforcement agencies, but the prohibition was overtaken by events and quickly eroded.

Evidence versus Intelligence

With the start of World War II, FBI Director J. Edgar Hoover, citing the danger of spies and other subversives, pressed to have Attorney General Robert Jackson's anti-wiretapping order overturned (Morgenthau, May 21, 1940). In view of the Supreme Court's *Nardone* decisions, this would take some fancy footwork. But, under Jackson, the Department of Justice had interpreted the *Nardone* decisions to mean that it was unlawful to both "intercept" *and* "divulge" communications, and had decided that it was not unlawful to intercept communications as long as the contents were kept within the federal government (USSR 94 *Intelligence Activities:*

Staff Reports, p. 278). Hoover urged President Roosevelt to authorize wiretapping for what we have come to call national-security purposes. The president acceded to Hoover's request, but his order stopped short of giving the FBI blanket approval to wiretap:

> I am convinced that the Supreme Court never intended any dictum in the particular case which it decided to apply to grave matters involving the defense of the nation....
>
> You are therefore authorized and directed in such cases as you may approve, after investigation of the need in each case, to authorize the necessary investigative agencies that they are at liberty to secure information by listening devices ... of persons suspected of subversive activities against the government of the United States, including suspected spies. You are requested furthermore to limit these investigations so conducted to a minimum and to limit them insofar as possible to aliens. (Roosevelt 1940)

Jackson, who wanted no part in wiretapping, made a fateful decision in response to the presidential directive: he instructed Hoover to maintain the records of all wiretaps, listing times, places, and cases (Theoharis and Cox 1988, p. 171). In so doing, Jackson effectively permitted the FBI to use wiretapping, free of Department of Justice oversight.

In 1941, Francis Biddle, the succeeding Attorney General, wrested back control of wiretaps from Hoover and turned down applications he felt were unjustified (Biddle 1941; USSR 94 *Intelligence Activities: Rights of Americans*, p. 37). In 1952, Attorney General J. Howard McGrath, in a letter to Hoover supporting the use of wiretaps "under the present highly restrictive basis," made explicit the requirement that all FBI wiretaps required the attorney general's prior approval (McGrath 1952). However, McGrath did not undo the custom that surveillance orders operated without time limits. Only in 1965, when Attorney General Nicholas Katzenbach recommended that authorizations be limited to 6 months (Hoover 1965), did the FBI change its practice.

In 1940 and 1941, several bills that attempted to establish a legal basis for electronic surveillance were introduced in Congress. One of these was endorsed by Roosevelt and Jackson (USSR 94 *Intelligence Activities: Staff Reports*, p. 280), but Hoover opposed any legislation requiring warrants for wiretapping (Hoover 1941) and no legislation passed.

When the war ended, Hoover sought and received continued wiretapping authority from President Harry Truman. Indeed, the power was broadened. In his reauthorization request to Attorney General Thomas Clark, Hoover omitted the final sentence of Roosevelt's original memo, which had required that electronic surveillance be kept to a minimum and limited "insofar as possible to aliens" (Gentry 1991, p. 324). Clark forwarded the amended memo and urged Truman to approve wiretapping in cases "vitally affecting domestic security, or where human life is in jeopardy," and Truman apparently signed it without being aware of the shift from earlier policies (Clark 1946).

In time Truman's aides discovered the change. A 1950 memo to Truman from George Elsey, assistant counsel to the president, reported that "not only did Clark fail to inform the President that Mr. Roosevelt had directed the FBI to hold its wiretapping to a minimum . . . he requested the President to approve very broad language [that was] a very far cry from the 1940 directive" (Elsey 1950). Truman, however, took no action to rescind the expanded authority. The new authorization meant that national security was no longer the sole justification for wiretaps (Clark 1946).

By adding "domestic security" to the list of reasons for which wiretapping could be employed, Clark's memo substantially broadened Roosevelt's directive. Developing intelligence is quite different from collecting evidence. In particular, intelligence investigations have less narrowly defined goals than criminal investigations. Developing intelligence is neither attempting to find evidence of a specific crime nor developing a case against a specific suspect. Rather, it is attempting to discern a pattern of behavior: What is the structure of an organization? What are its goals? What are its methods?

Those who work in intelligence emphasize the degree to which they operate under legal restraints intended to protect the rights of Americans. Yet the very character of intelligence work makes it unlikely that these restraints weigh as heavily on them as on criminal investigators. Intelligence officers don't go into court to face opposing attorneys. Criminal investigations are unsuccessful without convictions. Intelligence investigations—even in counterintelligence, where prosecution is sometimes

appropriate—can be deemed successful even if no prosecutions occur. The changes Clark made were thus quite significant. They moved wiretap investigations into a shadowy area where, by and large, they were protected from public scrutiny.

Since the two *Nardone* rulings made both evidence from federal wiretaps and evidence tainted by federal wiretaps inadmissible in court, the Department of Justice believed that if wiretapping had been used in a case, it could not prosecute. This eventually gave rise to an elaborate FBI methodology for concealing evidence of wiretapping.

In 1949, Judith Coplon, a Department of Justice employee, was caught as she was about to hand over 28 confidential FBI documents to Valentin Gubitchev, a Soviet employed by the United Nations. Hoover sought to prevent the documents—which revealed FBI wiretapping of Coplon—from appearing at Coplon's trial, but the judge ruled that the government had to release copies to the court. Fearing public disclosure of the FBI's wiretapping practices, Hoover tried to persuade the attorney general to drop the charges against Coplon, but without success. Hoover responded with new procedures regarding wiretapping. FBI reports of "highly confidential" sources, including wiretaps, would not be included in the main case files; instead they would be kept in especially confidential files (FBI 1949).[4]

A second trial revealed that Coplon herself had been wiretapped, despite denials by an agent who turned out to have read the transcripts. Hoover then went to even greater lengths to hide the paper trail between wiretaps and their logs. Agents working on a case were kept in the dark about any associated wiretaps so that they could not even accidentally reveal wiretap information in court. Hoover accomplished this by disguising information derived from wiretaps when it appeared in the case files. He was largely successful in this strategy, but he hoped for looser rules regarding wiretaps.

In 1954, President Dwight Eisenhower's attorney general, Herbert Brownell, was pressing for legislation to permit warrantless wiretapping as an aid in prosecuting communists. "You can't trust a Communist to tell the truth on the witness stand," Brownell (1954a, p. 202) argued, "and you can't trust the courts not to leak information about wiretap

applications." Brownell was frustrated because there was "evidence in the hands of the Department as a result of investigations conducted by the FBI which would prove espionage in certain ... cases." He argued that a change in the wiretap law would enable the Department of Justice to prosecute certain cases that it was currently prevented from pursuing (ibid., p. 203).

The House Judiciary Committee accepted Brownell's argument and recommended passage of legislation permitting warrantless wiretapping, but the full House of Representatives disagreed (USSR 94 *Intelligence Activities: Staff Reports*, p. 284). The legislation was amended to require a warrant, but this version did not receive support from the Department of Justice and died (ibid.). Although Congress periodically considered legislation on wiretapping, there were no new federal laws on the subject until the 1960s.

Meanwhile, as a result of the Federal Communications Act's prohibition against "interception and divulgence" of wired communications, wiretaps were useless as court evidence. As Attorney General put it to Congress in 1965:

> I think perhaps the record ought to show that when you talk national security cases, they are not really cases, because as I have said repeatedly, once you put a wiretap on or an illegal device of any kind, the possibilities of prosecution are gone. It is just like a grant of immunity.... I have dismissed cases or failed to bring cases within that area because some of the information did come from wiretaps. But here we feel that the intelligence and the preventive aspect outweigh the desirability of prosecution in rare and exceptional circumstances. (USSH 89 *Invasions of Privacy*, p. 1163)

In 1950, and again in 1953, presidential directives authorized the FBI to investigate "subversive activity" (USSR 94 *Intelligence Activities: Rights of Americans*, p. 45). Since these directives failed to provide guidelines for such investigations, the FBI took a very broad view of what constituted subversive activity. Surveillance, often including wiretapping and electronic bugging, was not limited to those suspected of crimes or even to detecting suspected criminal activities.

Though many other types of domestic activities were the targets of surveillance, Hoover stressed the danger of Communist subversion, and the FBI collected intelligence about the influence of Communists in a va-

riety of categories, including "political activities, Negro question, youth matters, women's matters, farmers' matters, veterans' matters" (FBI 1960a).

Believing that the growing civil rights movement was Communist inspired and would lead to violence, Hoover kept it under careful observation. In 1956 he briefed a cabinet meeting about the Communists' "efforts" and "plans" to influence the movement. This briefing demonstrates how far the FBI overreached its mandate in internal security investigations. Not limiting his discussion to the possibility of violence, Hoover went on to present to the cabinet the legislative strategy of the NAACP and "the activities of Southern Governors and Congressmen on behalf of groups opposing integration peacefully" (FBI 1956).

Permission to conduct investigations of domestic "subversive activity" without restraint gave the FBI free rein in collecting wide-ranging domestic intelligence. The FBI's choice of electronic surveillance as the means for doing this allowed it to keep its activities hidden and uncontrolled for a long time. An official of the Nation of Islam was wiretapped for 8 years without any efforts to prosecute him for illegal activities (Hoover 1956), and the Socialist Workers Party was the target of FBI wiretaps and bugs for 20 years.

The extent of the FBI's wiretapping under J. Edgar Hoover has never been clear.[5] Although Congress received annual testimony from Hoover, it was unable to discover how much wiretapping was actually occurring, since the figures Hoover gave did not include the taps installed by field agents on their own or the taps installed by local police at the FBI's request.

Hoover kept the transcripts of wiretaps—many of them hidden in obscure files—even when they revealed no evidence of criminal activity. Since wiretaps on suspected spies and organized crime figures sometimes picked up conversations with politicians or other influential people, Hoover developed a mass of material with great political value. This is how he ended up with transcripts of intimate conversations between John Kennedy and Inga Arvad, a Danish reporter and former Miss Europe who had visited Germany for social functions with high Third Reich officials, including Hitler. The FBI was investigating allegations that Arvad was a German spy (Anderson 1996a, pp. 48–52). The investigation itself

may have been legitimate. The recordings were made during the World War II, while Kennedy was a Naval officer. Nonetheless, although the investigation produced no evidence of espionage, recordings of his pillow talk with Arvad were still in the FBI files when Kennedy became president nearly 20 years later.

It is believed that, without any pretense of investigating criminal activities, Hoover wiretapped senators and congressmen.[6] It is known that he wiretapped various Supreme Court justices.[7] The existence of extensive records on political figures was well known, and these files ensured that Hoover got much of what he wanted. Congress exercised little oversight of the FBI's affairs, wiretapping included.

One example is particularly illustrative of the way in which Hoover was able to use the FBI's investigative powers to protect its interests. In 1965, a Senate subcommittee undertook an investigation of electronic surveillance and mail covers. The FBI, a major focus of this review, was concerned. One FBI memo noted: "Senator Long ... has been taking testimony in connection with mail covers, wiretapping, and various snooping devices on the part of federal agencies. He cannot be trusted." (Jones 1965) Two high-ranking Bureau officials met with Edward Long (the chairman of the subcommittee) and a committee counsel. There is no indication that there were any briefings of other subcommittee members, nor is there any reason to believe that during the 90-minute meeting Long was told any details of FBI electronic surveillance, such as the bugging of a congressman's hotel room during the sugar lobby investigations (see below), the bugging and wiretapping of Martin Luther King, or the wiretapping of a congressional staffer, two newspaper reporters, and an editor of an anti-Communist newsletter (USSR 94 *Intelligence Activities: Staff Reports*, p. 309). The FBI men suggested that the senator issue a statement saying that he had held lengthy conferences with FBI officials and was now completely satisfied "that the FBI had never participated in uncontrolled usage of wiretaps or microphones and that FBI usage of such devices has been completely justified in all cases" (DeLoach 1966a). When Long said that he did not know how to write such a press release, the FBI officials said they would be happy to do so—and they did (ibid.).

The Long Subcommittee chose not to hold hearings on FBI electronic-surveillance practices. An internal FBI memo noted: "While we have neu-

tralized the threat of being embarrassed by the Long Subcommittee, we have not eliminated certain dangers which might be created as a result of newspaper pressures on Long. We therefore must keep on top of this situation at all times." (DeLoach 1966b) The FBI's determination to control such investigations can be inferred from the fact that it maintained files on all members of the subcommittee (USSH 94 *Intelligence Activities: FBI*, p. 477).

A year later Senator Long again took up the fight, introducing a bill to limit FBI electronic surveillance to national-security cases. Hoover was not pleased. Shortly afterwards *Life* broke a story that the senator had received $48,000 from Morris Shenker, Jimmy Hoffa's counsel (Lambert 1967). The article intimated that the money was a bribe to prevent or reverse charges against the Teamsters' leader. The senator's career ended, and his electronic-surveillance bill died.

Hoover remained firmly in power through eight presidencies and 48 years. His long tenure as director is now recognized as a period during which the FBI routinely engaged in the sort of widespread political surveillance usually associated with totalitarian regimes.

In part Hoover's control came about because of abdication of responsibility by other members of the government. Truman's 1946 authorization of wiretaps in investigating subversive activities required the attorney general to authorize their use. There were, however, many occasions on which an attorney general was informed of the wiretaps only after they had been installed (USSR 94 *Intelligence Activities: Rights of Americans*, p. 63). In 1965, under a directive from President Johnson, Attorney General Katzenbach tightened requirements for electronic surveillance. By then Johnson opposed wiretapping except in cases of national security, and in a directive that went out to heads of agencies he wrote: "In my view, the invasion of privacy of communications is a highly offensive practice which should be engaged in only where the national security is at stake." (Johnson 1965) Installation of bugs now needed written approval from the attorney general, and both bugs and wiretaps were subject to 6-month time limits, after which new authorization from the attorney general was required (USSR 94 *Intelligence Activities: Rights of Americans*, p. 105).

Even with the tightened restrictions, the Department of Justice did not feel that it controlled the FBI's use of wiretapping. In 1972, former Attorney General Ramsey Clark told a judge: "Reports by FBI agents on electronic surveillance had caused the Department [of Justice] 'deep embarrassment' many times. Often we would go to court and say that there had been no electronic surveillance and then we would find out we had been wrong. Often you could not find out what was going on ... frequently agents lost the facts." (Theoharis 1974, p. 342)

The FBI was not the only law-enforcement agency to engage in wiretapping without regard for the views of legislators and judges. State police also wiretapped, sometimes legally, sometimes not.

Wiretapping was made illegal in Illinois in 1927, but Chicago's police intelligence unit ignored the law. The police saw no reason to try and change the legislation; the effort would only raise controversy. They merely continued wiretapping, aware that their actions were illegal (Dash et al. 1959, p. 222).

In California, wiretaps were similarly banned, but the police there took a different tack. When law-enforcement officers wanted to do a wiretap investigation, they would hire a private investigator, who was told to deny any official connections if caught in the act of tapping (ibid., pp. 164–165).

Even in states that permitted police wiretapping, numbers could be misleading. Official records in the State of New York showed fewer than 3,000 wiretap orders for the period between 1950 and 1955. A careful study by Samuel Dash and his two co-authors led to different conclusions. They observed that the official figures omitted wiretaps installed by plainclothesmen. Those numbers were surprisingly large. Dash et al. (ibid., p. 68) concluded that for every 10 wiretaps installed by plainclothesmen who had obtained court orders, another 90 taps were installed without court authorization. This interpretation would indicate that the New York police performed between 16,000 and 29,000 wiretaps a year.

Oddly enough, in Massachusetts, a state with a particularly liberal wiretapping law that required only written permission from the attorney general or the district attorney, the Boston Police Department did not use

wiretaps in criminal investigations. The public was opposed to it, and the police believed wiretapping was a "dirty business" to which "only a lazy police department" would resort (Dash et al. 1959, p. 147).

Wiretaps versus Bugs

Microphone surveillance and wiretapping play similar investigative roles. But the Federal Communications Act said nothing about microphone surveillances, and the *Nardone* decisions therefore left such bugging legal. Although ultimately the Supreme Court whittled away at the warrantless use of electronic bugs, its early decisions condoned the practice.

In 1942 the Supreme Court ruled that it was legally permissible for law-enforcement officers to plant a bugging device on a wall adjoining that of a suspect's office (*Goldman v. United States*, 316 US 129). In 1954 it upheld a state court conviction based on evidence obtained by microphones concealed in walls of the defendants' homes during warrantless break-ins by the police (*Irvine v. California*, 347 US 128).

In *Irvine*, in sharp contrast to later decisions, the Supreme Court ruled that, because the case in question had been a state prosecution within a state court, the conviction could stand. Members of the Court were disturbed, however, by violations of the Fourth and Fifth Amendments. The bug had been placed in a bedroom, and the justices were deeply offended by the invasion of privacy. Attorney General Herbert Brownell "clarified" policy for J. Edgar Hoover, warning that the language of the Court "indicates certain uses of microphones which it would be well to avoid" because "the Justices of the Supreme Court were outraged by what they regarded as the indecency of installing a microphone in the bedroom" (Brownell 1954b).

In 1961, in *Julius Silverman et al. v. United States* (365 US 505), the Supreme Court changed its direction, holding that a search occurred whenever a bug was used, even if the walls of the target's apartment had not been breached. The case arose when District of Columbia police, suspecting that gambling was taking place in a row house, pushed a foot-long "spike mike" into a space under the suspect's apartment from the vacant house next door. The spike hit a solid object (most likely a heating duct), which "became in effect a giant microphone" (ibid., p. 509).

Telephone conversations were picked up from the room above, amplified, and taped. The Court held that, in the absence of a search warrant, the evidence was inadmissible. In the *Nardone* cases, the Court had ruled on the narrow basis of the FCA. In *Silverman*, it brushed away these technicalities ("In these circumstances we need not pause to consider whether or not there was a technical trespass under the local property law relating to party walls" (ibid., p. 511)) and ruled on the basis of the Fourth Amendment. With this decision, the Court began moving in the direction of constitutional protection against warrantless electronic surveillance.

In 1967, the Supreme Court established the doctrine of "legitimate expectation of privacy." In *Charles Katz v. United States*, (389 US 347) the Court determined that evidence obtained from a warrantless electronic bug placed in a public phone booth was inadmissible:

> . . . [W]hat [Katz] sought to exclude when he entered the [telephone] booth was not the intruding eye—it was the uninvited ear. . . . No less than an individual in a business office, in a friend's apartment, or in a taxicab, a person in a telephone booth may rely upon the protection of the Fourth Amendment. One who occupies it, shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world. To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication. (ibid., pp. 511–512)
>
> . . . Wherever a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures. (ibid., p. 515)

With this decision, the Supreme Court changed the doctrine underlying US wiretap law. Unlike the *Nardone* decisions, which relied on statutory interpretation, *Katz* is based on underlying principles of the Constitution. In ruling that electronic bugging was illegal without a search warrant, the Supreme Court arrived at the current view of bugs and wiretaps as a form of search: that they are permissible, but subject to the limitations and protections laid down in the Fourth Amendment.

Wiretapping and Organized Crime

When asked to explain the need for wiretapping, police often cite organized crime as the principal application. In order to attack organized

crime, police must find a way of penetrating the tightly knit organizations. This is not easy. The difficulty is compounded by the fact that "the core of organized crime activity is the supplying of illegal goods and services . . . to countless numbers of citizen customers" (President's Commission on Law Enforcement 1967, p. 187), and the consensual nature of these crimes means that "law enforcement lacks its staunchest ally, the victim" (Duke and Gross 1993, p. 107). Organized crime is particularly effective in using the code of *omerta*—silence—to keep its participants and its victims from speaking to law-enforcement agents (ibid., p. 198). A common police response has been the use of electronic surveillance. The 1967 *Katz* decision took this tool from the police just as the visibility of organized crime was increasing.

Organized crime had been a force in American society for years. With the repeal of Prohibition, it had shifted its activities from bootlegging into gambling, loansharking, and control of legitimate businesses, including garbage disposal, garment manufacturing, real estate, restaurants, vending machines, and waterfront activities (ibid., p. 195). Yet between the 1930s and the 1950s the FBI pursued bank robbers, kidnappers, auto thieves, and the Communist Party, but not organized crime (although from time to time individual members of crime "families" made their way into the FBI's net).

There are various theories as to why J. Edgar Hoover ignored organized crime's very existence for some 30 years. It may be that any concerted federal effort would have involved the FBI in interagency cooperation, something that the turf-conscious Hoover abhorred. It may be that an investigation of organized crime would have been a drawn-out affair that would not have yielded the statistics on criminals caught and property recovered that were the "heart and soul" of Hoover's annual speech before the Senate Appropriations Committee (Sullivan 1979, pp. 117–118). It may be that investigating organized crime would have risked corruption of the investigators to a much greater extent than other types of criminal investigation.

Organized Crime Becomes Visible

Sergeant Edgar Croswell, a New York State trooper, Robert Kennedy, Attorney General under his brother John, and Joseph Valachi, a 60-year-

old "soldato" in the Genovese crime family, brought organized crime to the nation's attention in the late 1950s and the early 1960s.

On Saturday November 15, 1957, Sergeant Croswell was doing his morning rounds in Apalachin, a small village in the Southern Tier of New York State, near Pennsylvania, when he discovered limousine after black limousine turning into the country estate of Joseph Barbara, a bottler and distributor of soft drinks in nearby Endicott. His suspicion aroused, Croswell set up a roadblock near the estate to check for vehicle identification—a legal search under the state laws. Many of the crime bosses fled, but 67 of them were identified—some through the roadblock, others through various forms of carelessness, including registering under their own names at hotels in the area. The next day, the nation awoke to headlines like "Royal Clambake for Underworld Cooled by Police" and "Police Ponder NY Mob Meeting; All Claim They Were Visiting Sick Friend."

In 1961 Robert Kennedy became US attorney general. Five years earlier, while counsel to the Senate Select Committee on Improper Activities in the Labor or Management Field, Kennedy had investigated labor racketeering and had uncovered ties between the unions and organized crime. When he became attorney general, Kennedy made organized crime a priority (Lewis 1961). Congress soon passed legislation that Kennedy had requested to fight organized crime (*New York Times* 1961).

In 1963, Joseph Valachi broke the code of silence that had made investigations of organized crime so unrewarding. Imprisoned for heroin trafficking, Valachi killed a man whom he believed had been sent to assassinate him in jail. Soured by the belief that the "family" had tried to have him "hit" and facing murder charges for defending himself, Valachi turned government witness and began to talk. In the Senate's staid hearing rooms, Valachi laid out the complex system of bosses, soldiers, and international links that characterized organized crime. Charts describing the succession of gang control in the New York area graced the walls. The information was shocking to those who had been repeatedly told by the FBI's director that organized crime did not exist.

The combined effect was to transform organized crime from a myth to a priority in federal eyes. The government concluded that its involvement was crucial in working against organized crime because criminal

networks flourished largely as a result of corruption in local police forces. In the words of Ramsey Clark, Kennedy's successor as attorney general: "The presence of any significant organized crime necessarily means that local criminal justice has been corrupted to some degree." (Clark 1970) Furthermore, because the criminal organizations spanned state borders, nationwide coordination of investigations was viewed as crucial.

By 1966, even J. Edgar Hoover had caught up on organized crime. Testifying before the House Subcommittee on Appropriations, Hoover said: "La Cosa Nostra is the largest organization of the criminal underworld in this country, very closely organized and strictly disciplined." (Carroll 1967)

Title III: Wiretaps Made Legal

In their report on the Valachi hearings, members of the Senate Governmental Operations Committee called for legislation authorizing wiretapping. Their view was echoed by a presidential commission on law enforcement: "A majority of the members of the Commission believe that legislation should be enacted granting carefully circumscribed authority for electronic surveillance to law enforcement officers. . . ." (President's Commission on Law Enforcement 1967, p. 203)

Not all experts agreed with the commission's conclusions. Attorney General Clark prohibited all use of wiretaps by federal law-enforcement officers. He told Congress: "I know of no Federal conviction based upon any wiretapping or electronic surveillance, and there have been a lot of big ones. . . . I also think that we make cases effectively without wiretapping or electronic surveillance. I think it may well be that with the commitment of the same manpower to other techniques, even more convictions could be secured, because in terms of manpower, wiretapping, and electronic surveillance is very expensive." (Clark 1967, p. 320) Clark pointed out that in 1967, without using wiretaps, federal strike forces had obtained indictments against organized crime figures in nine states, and that "each strike force has obtained more indictments in its target city than all federal indictments in the nation against organized crime in as recent a year as 1960" (ibid., pp. 79–80).

In 1965, the Chief Judge of the US District Court in Northern Illinois,

William Campbell, told Congress of his strong disapproval of wiretaps: "My experiences have produced in me a complete repugnance, opposition, and disapproval of wiretapping, regardless of circumstances. This invasion of privacy, too often an invasion of the privacy of innocent individuals, is not justified. In every case I know of where wiretapping has been used, the case could have been made without the use of the wiretap. Wiretapping in my opinion is mainly a crutch or shortcut used by inefficient or lazy investigators." (USSR 90-1097 *Omnibus Safe Streets and Crime Control*, p. 1495)

Detroit's police commissioner, Ray Girardin, was also opposed to wiretapping: "I feel that [wiretapping] is an outrageous tactic and that it is not necessary and has no place in law enforcement.... [T]he only exception to this that I would entertain at this time would be in a situation where the security of the nation has to be protected against an outside power." (Girardin 1967)

At other times, in other places, other officials had denounced wiretapping. A 1961 congressional survey revealed that the attorneys general of California, Delaware, Missouri, and New Mexico opposed federal laws permitting wiretapping (USSH 87 *Wiretapping and Eavesdropping Legislation*, pp. 545, 547, 554, and 560). Daniel Ward, State's Attorney for Cook County, Illinois, testified in 1961: "I do not think that one can honestly say that wiretapping is a *sine qua non* of effective law enforcement." (Ward 1961)

Ramsey Clark's opposition was sustained by President Johnson, who proposed to Congress in 1967 that wiretapping be limited to national-security cases and that it be performed only by federal officials (*Congressional Quarterly Weekly* 1967, p. 222). But in the aftermath of the Crime Commission's report, and during a time of domestic unrest (riots in the ghettos, the Vietnam War protests, and several political assassinations), Congress saw the issues differently. Despite the lack of unanimity, even among police, Congress chose to legalize wiretapping as a tool for law-enforcement investigations in criminal cases. Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (18 USC §2510–2521) established the basic law for interceptions performed in criminal investigations: wiretaps are limited to the crimes specified in the act—a list including murder, kidnapping, extortion, gambling, counterfeiting, and

sale of marijuana. The Judiciary Committee made clear that organized crime was a central motivation for Title III.[8]

In order to conform to the standards of the Fourth Amendment, Congress required law enforcement to obtain a warrant before initiating a wiretap.[9] To receive a court order, an investigator draws up an affidavit showing that there is probable cause to believe that the targeted communication device—whether a phone, a fax, or a computer[10]—is being used to facilitate a crime. A government attorney prepares an application for a court order, and approval must be granted by a member of the Department of Justice at least at the level of Deputy Assistant Attorney General.

Observing that "wiretaps and eavesdrops are potentially more penetrating, less discriminating, and less visible than ordinary searches," Congress decided that review of the application by a federal district court judge was in order (National Commission 1976, p. 12). The judge must determine that (i) there is probable cause to believe that an individual is committing or is about to commit an indictable offense; (ii) there is probable cause to believe that communications about the offense will be obtained through the interception; (iii) normal investigative procedures have been tried and either have failed, appear unlikely to succeed, or are too dangerous; and (iv) there is probable cause to believe that the facilities subject to surveillance are being used or will be used in the commission of the crime. Only if all these criteria are satisfied will a judge approve a wiretap order.[11]

After a court order for electronic surveillance is approved, it is taken to a service provider (e.g., a telephone company) for execution. The provider is required to assist in placing the wiretap,[12] and is compensated for all expenses. Surveillances are approved for at most 30 days; any extension requires a new court order.

Almost all states have also passed statutes permitting wiretaps by state and local law enforcement officers for criminal investigations. Under Title III, state acts were required to be at least as restrictive in their requirements as the federal code, and many are more so.

In an effort to prevent repetition of the concealment practiced by J. Edgar Hoover, Congress required that records on electronic surveillance be available to the public. Each order, whether filed under Title III or

under a state statute, must be reported, and every year the Administrative Office of the United States Courts issues a report detailing the duration of each order, the number of persons intercepted, the type of surveillance used, the outcome of the case, and other information.

A New Wrinkle: "Domestic National Security"

There are different codes of conduct in wartime than in peacetime. Soldiers are permitted, under appropriate circumstances, to kill without the elaborate procedures required for a civil execution. The most common "appropriate circumstance" is, of course, war with a foreign power. Less commonly and more controversially, a country's military may be deployed against its own citizens in times of insurrection. Under these conditions, which constitute a threat to the state itself, it is generally felt that peacetime restraint would place the state at too great a disadvantage and permit the country to be conquered or the government to be overthrown.

Similar reasoning applies, even in peacetime, to the state's actions with respect to spies, subversives, and revolutionaries—people who are not, or do not consider themselves, bound by the country's laws. The state will, where possible and appropriate, treat such people as lawbreakers and prosecute, but it may also take other actions that are not taken against citizens in the normal course of events.

It is not surprising, therefore, that in matters affecting national security the legal requirements for the placement of wiretaps should be relaxed. This is the reasoning behind the 1940 authorization granted to J. Edgar Hoover by Franklin Roosevelt. In a more general sense, it is the reasoning under which all intelligence agencies conduct communications intercept operations against foreign targets.

The relaxed requirements for national-security wiretapping are an attractive target for abuse. A number of presidents, including Kennedy, Johnson, and Nixon, used "national security" as a pretext for employing wiretaps in domestic political intelligence.

Kennedy abused electronic surveillance only a month into his presidency. The Dominican Republic was pressing Congress to pass a bill that would allow more Dominican sugar to be imported. Kennedy opposed

this legislation, and his administration suspected that congressmen were being bribed to support it. Such bribery would be a legitimate national-security concern. Attorney General Robert Kennedy requested that the FBI initiate an investigation to see what pressures the Dominican Republic was putting on Congress (Wannall 1966). The inquiry lasted 9 weeks. A dozen wiretaps and three microphone surveillances were involved. Three members of the Department of Agriculture and a Congressional staffer had their home phones tapped (Hoover 1961a,b). One lobbyist was wiretapped both at home and at the office (Hoover 1961b). No bribes were discovered, but the wiretaps provided the president with important political information. One FBI summary sent to the attorney general said that a lobbyist "mentioned he is working on the Senate and has the Republicans all lined up" (FBI 1962). The administration bill won, and the FBI concluded that its surveillance work had been a major factor (Wannall 1966). Most of the wiretaps were taken off in April 1961, but two remained even after the administration's bill passed (USSR 94 *Intelligence Activities: Staff Reports*, p. 330).

President Lyndon Johnson was even more blatant in requesting national-security wiretaps. During the 1968 election, Johnson (who was not a candidate for reelection) asked the FBI to conduct surveillance of Anna Chennault, a prominent Republican who, Johnson claimed, was attempting to undermine the US-Vietnam peace talks in Paris. The White House asked the FBI to institute physical coverage of Chennault and both physical and electronic coverage of South Vietnam's Embassy (USSR 94 *Intelligence Activities: Staff Reports*, p. 314). Summaries of the information obtained from the physical surveillance were later given to the White House (DeLoach 1968b; FBI 1968). Apparently the FBI was concerned about being involved in such a political case and eschewed electronic surveillance of Chennault. The electronic surveillance of the embassy was an indirect way of accomplishing the same goal (DeLoach 1968a; USSR 94 *Intelligence Activities: Staff Reports*, p. 315).

President Nixon went yet further, and ultimately the illegal electronic surveillance that started early in his administration played a pivotal role in toppling his presidency.

On May 9, 1969, a front-page story appeared in the *New York Times* reporting that the United States was bombing Cambodia and had been

doing so for some time. By recording false coordinates for the sorties (placing them in South Vietnam), the Air Force had hidden the location of the attacks. News of the cover-up had been leaked to *Times* reporter William Beecher by someone in the government. Outraged, Henry Kissinger, Nixon's national security advisor, told J. Edgar Hoover to find the leaker(s). Within hours the FBI had focused on Morton Halperin, a Kissinger aide who "knew Beecher" and whom Hoover "considered part of the Harvard clique" (Hoover 1969a). Without written approval from the attorney general, a wiretap was installed on Halperin's home line that same afternoon. Seventeen people, some in the government and some in the news media, had their phones tapped during the investigation,[13] but no leakers were identified.

Some of the wiretaps were on for a matter of weeks, others for more than a year. The longest was the one on Morton Halperin, which remained active for 21 months, even though by September 1969 Halperin had left the White House. In February 1971, when the tap was finally removed, Halperin had been working for months for Edmund Muskie, a Democratic senator from Maine and a candidate for his party's presidential nomination (Halperin 1974, p. 296). Hoover was forwarding various tidbits of political information, such as the fact that former president Johnson "would not back Muskie" for the White House (Theoharis and Cox 1988, p. 415). By that time, information from the wiretaps was being sent directly to H. R. Haldeman, Nixon's political advisor (USSR 93 *Electronic Surveillance for National Security*, pp. 296 and 351).

Daniel Ellsberg's turn came next. Ellsberg had made copies of classified histories of US involvement in Vietnam—the 47-volume "Pentagon Papers"—available to *New York Times* reporter Neil Sheehan. On Sunday, June 13, 1971, portions of the papers, and articles based on them, began appearing in the *Times*. The government sued to block publication, but lost. Excerpts were printed in the *Times* and in the *Washington Post*.[14]

Although the Pentagon Papers were highly critical of the Democrats who had preceded him in the presidency, Nixon was infuriated by their publication. Ellsberg was indicted on charges of violating the Espionage Act, but the Nixon White House went further.

John Ehrlichman, Nixon's domestic affairs advisor, authorized a burglary of Ellsberg's psychiatrist, then covered it up in an attempt to keep

Ellsberg's trial from ending in a dismissal of charges. Instead, as a result of the inquiries into the Watergate break-in, the burglary of the psychiatrist was discovered. Further inquiry revealed that Ellsberg's phone had been tapped by the government,[15] but the wiretap authorizations, logs, and other records could not be found. The judge declared a mistrial, and charges against Ellsberg were dismissed (*United States v. Susso*, CD Cal. 9373-WMB, 1973).

Charles Radford II, a Navy yeoman who was serving the Joint Chiefs of Staff, was wiretapped after a syndicated newspaper column by Jack Anderson described a conversation between Nixon and Kissinger concerning the administration's decision to "tilt" toward Pakistan in the India-Pakistan conflict—a column which was to contribute to Anderson's winning a Pulitzer Prize a few months later. Radford was a suspect in part because he and Anderson attended the same church (Smith 1973; Hersh 1983, p. 470). The FBI was asked to wiretap Radford, although the government did not plan any prosecution of the leak (Smith 1973). Shortly afterward, Radford was transferred to the Naval Reserve Training Center near Portland, Oregon. He moved in with his stepfather until he could find permanent housing. A wiretap was put on the stepfather's phone. After Radford found a place of his own, a wiretap was placed on his new phone. The wiretap on the stepfather's phone remained for another 2 months. There were also wiretaps on the phones of two of Radford's friends, one a State Department employee and one a former Defense Attaché. None of the wiretaps were authorized by the attorney general, and at no time was prosecution planned (USSR 94 *Intelligence Activities: Staff Reports*, pp. 326–327).

Wiretapping Requires a Court Order

Even after the Supreme Court's ruling in the *Katz* case and the passage of Title III, national security continued to serve as a cover for warrantless electronic surveillance in domestic political intelligence. In 1972 the Supreme Court ordered an end to warrantless wiretapping even for "national-security" purposes.

John Sinclair, Lawrence Plamondon, and John Waterhouse Forrest were charged with bombing a CIA office in Ann Arbor, Michigan. It turned out that the federal government had tapped Plamondon without

prior judicial approval. Plamondon requested copies of the tapes to determine if the government's case had been tainted by the wiretaps. The District Court ordered the government to give Plamondon copies of the tapes.

The government refused and appealed. It argued before the Supreme Court that this was a matter of national security and that Title III requirements for a search warrant were not an attempt to limit surveillance in such cases. While the Supreme Court agreed that Title III was limited to criminal investigations, it did not buy the argument that domestic-security surveillance could justify departure from Fourth Amendment protections:

> . . . these Fourth Amendment freedoms cannot be properly guaranteed if domestic security surveillances may be conducted solely within the discretion of the Executive Branch. . . . (*United States v. United States District Court for the Eastern District of Michigan et al.*, 407 US 297, 1972, p. 316–317)

> Official surveillance, whether its purpose be criminal investigation or ongoing intelligence gathering, risks infringement of constitutionally protected privacy of speech. Security surveillances are especially sensitive because of the inherent vagueness of the domestic security concept. . . . We recognize, as we have before, the constitutional basis of the President's domestic security role, but we think it must be exercised in a manner compatible with the Fourth Amendment. . . .
>
> We cannot accept the Government's argument that internal security matters are too subtle and complex for judicial evaluation. Courts regularly deal with the most difficult issues of our society. . . . If the threat is too subtle or complex for our senior law enforcement officers to convey its significance to a court, one may question whether there is probable cause for surveillance. . . . (ibid., p. 320)

Surveillance of domestic organizations now required a court order whether the national security was involved or not. The Court pointed to the absence of law on wiretapping for national-security purposes and invited Congress to fill the gap. Instead the country spent almost 2 years mesmerized by the president's illegal activities.

Watergate

The Watergate affair began early on the morning of June 17, 1972, with a break-in at the Democratic National Committee's headquarters in the

Watergate Office Building in Washington. The intruders were a group paid by the Committee to Re-Elect the President, Nixon's campaign committee. The burglary was the second attempt to install a bug on the phone of Lawrence O'Brien, the Democratic Party's chairman. A first attempt had only succeeded in placing a working bug in his secretary's phone. This provided information on the secretary's social life, but not on O'Brien's political plans.

The Watergate affair reached its climax on August 9, 1974, when Nixon, facing impeachment, became the first president to resign from office. Had he not done so, he could have expected to be impeached on counts that included the following:

> [Nixon] misused the Federal Bureau of Investigation, the Secret Service, and other Executive Personnel ... by directing or authorizing such agencies or personnel to conduct or continue electronic surveillance or other investigations for purposes unrelated to national security, the enforcement of laws, or any other lawful function of his office; ... and he did direct the concealment of certain records made by the Federal Bureau of Investigation of electronic surveillance. (USHH 93 *Impeachment Inquiry*, Book III, pp. 2255–2256, Article II, §2)

> [Nixon] failed to take care that the laws were faithfully executed by failing to act when he knew or had reason to know that his close subordinates endeavored to impede and frustrate lawful inquiries ... concerning the electronic surveillance of private citizens.... (USHH 93 *Impeachment Inquiry*, Book III, pp. 2256–2258, Article II, §4)

The Senate Investigates

The revelations of Watergate engendered a general distrust of government as high official after high official was implicated in the illegal actions of the Nixon presidency. There was deep concern about the involvement of intelligence agencies in many of the questionable proceedings of the Nixon administration. In January 1975 the Senate appointed an eleven-member special committee to investigate government intelligence operations to determine the extent to which "illegal, improper, or unethical activities" were engaged in by government agencies (USS 94 *Resolution*).

The Senate Select Committee to Study Governmental Operations with respect to Intelligence Activities (commonly known as the Church Com-

mittee, after its chairman, Senator Frank Church), began its study with the year 1936, which marked the reestablishment of domestic intelligence programs in the United States after a hiatus of about a decade. The committee uncovered a long history of presidential wiretapping, including Truman's wiretapping of the lobbyist Thomas Corcoran, Kennedy's "Sugar Lobby" taps, Johnson's surveillance of Anna Chennault, and Kennedy's and Johnson's wiretapping and bugging of Martin Luther King. It also examined the wiretap abuses of the Nixon era, including those enumerated above. The hearings revealed many illegal covert operations by the intelligence agencies, and the Church Committee concluded:

> Too many people have been spied upon by too many Government agencies and [too] much information has been collected. The Government has often undertaken the secret surveillance of citizens on the basis of their political beliefs, even when those beliefs posed no threat of violence or illegal acts on the behalf of a foreign power. The Government, operating primarily through secret informants, but also using other intrusive techniques such as wiretaps, microphone "bugs," surreptitious mail opening, and break-ins, has swept in vast amounts of information about the personal lives, views and associations of American citizens.... (USSR 94 *Intelligence Activities: Rights of Americans*, p. 5)

Among these were "the interest of the wife of a US Senator in peace causes; a correspondent's report from Southeast Asia to his magazine in New York; an anti-war activist's request for a speaker in New York" (ibid., p. 108). The committee observed: "The surveillance which we investigated was not only vastly excessive in breadth ... but was also often conducted by illegal or improper means." (ibid., p. 12)

Although much of this surveillance had occurred before Title III, the illegal activities of the Nixon administration had not. When Congress had regulated the use of electronic surveillance for criminal investigations under Title III, it had believed that the legislation would put tight restrictions on the use of wiretaps and electronic surveillance. Nonetheless, Title III had been circumvented by the Nixon administration, which had used the "national-security" justification for many investigations.

The Church Committee's inquiries emphasized not "Who did it?" but "How did it happen and what can be done to keep it from happening again?" (ibid., p. viii) The committee felt that Title III was appropriate

as written, but set forth a list of recommendations for explicit laws on electronic surveillance in national-security investigations.[16]

The underlying premise of the Church Committee's recommendations was that Americans should be free of the type of surveillance the hearings had exposed. The CIA should refrain from electronic surveillances, unauthorized searches, or mail openings within the United States,[17] and NSA should not monitor communications from Americans, except in cases where the person is involved in terrorist activities or intelligence work, and then only when a search warrant has been obtained.[18] The committee also outlined the form a law permitting electronic surveillance for foreign intelligence might take. [19]

The Foreign Intelligence Surveillance Act

In 1978 the Foreign Intelligence Surveillance Act (FISA), much of it based on the Church Committee's recommendations, became law. FISA (50 USC 1801 et seq.) governs wire and electronic communications with "United States persons"[20] who are within the country. It does not apply to those of US persons overseas, excepting communications with a US person resident in the United States. Under FISA, US persons in the US may be subject to surveillance if they are suspected of aiding and abetting international terrorism.

A court order is required for a FISA wiretap.[21] Such an order may be granted by the Foreign Intelligence Surveillance Court, which is made up of eleven District Court judges specially appointed by the Chief Justice of the United States.[22] The order must be applied for by a federal officer, and approved by the attorney general, who is required to inform the House and Senate Committees on Intelligence of all FISA wiretap activity twice a year.

The attorney general is required to furnish an annual report to the Administrative Office of the US Courts on the number of FISA applications and orders. All other information on FISA wiretaps is classified. In that sense, FISA represented a move away from establishing public safeguards —notice to targets, oversight, and minimization (in FISA minimization is limited to minimization of information about US persons)—that both provide accountability and limit the ability to misuse surveillance authority.

For a long time after 1979, there were an average of slightly over 500 FISA wiretap orders per year[23]; by 1995, more than 8000 requests had been made by the government for surveillance under FISA. None had been turned down. The reason for this is a matter of dispute. Proponents of FISA say it is because surveillance applications are carefully prepared and reviewed before being presented to the Foreign Intelligence Surveillance Court. Opponents argue that it is because the court is only a rubber stamp (Cinquegrana 1989, p. 815). A critical report by the Foreign Intelligence Surveillance Court in 2002 shed a bit of light on these issues (see chapter 11).

The Electronic Communications Privacy Act

The next major federal wiretapping statute was the 1986 Electronic Communications Privacy Act (Public Law 99-508), which updated Title III to include digital and electronic communications. In recognition of new telecommunications switching technologies, ECPA allowed for approvals of *roving wiretaps*—wiretaps without specified locations—if there was demonstration of probable cause that the subject was attempting to evade surveillance by switching telephones. It required a warrant for wiretapping the non-radio portion of a cellular communication. The widespread availability of radio scanners made the latter stronger in legal terms than it was in practice.

Under ECPA, pen registers and trap-and-trace devices require court orders. Any government attorney can file for such an order, and there is no requirement of probable cause for a search warrant to be issued.

The late 1980s witnessed two major changes in telecommunications. The breakup of the Bell System into a long-distance carrier and seven regional companies encouraged a proliferation of competitors in the industry; this made seeking a wiretap more complicated for law-enforcement agents, who now had to contend with a plethora of new companies instead of a monolithic "Ma Bell." The other change came when call forwarding, call waiting, cellular phones, and fax machines appeared on the market.