Chapter 2

Introduction and Overview

Chapter 2
Introduction and Overview

SUMMARY

Electronic surveillance is the epitome of the two-edged sword of technology for many Americans. Public opinion polls evidence considerable concern about possible excessive and abusive use of electronic surveillance by the Government (and others), and show support for strong safeguards and protections to tightly control the use of such technology. But, at the same time, the public is concerned about crime—especially violent crime—and supports the appropriate use of technology to combat and prevent crime and bring offenders to justice. [1]

Until the past 10 years or so, the balancing of these concerns was relatively straightforward from a technological perspective. Electronic surveillance was limited primarily to audio surveillance devices such as telephone taps and concealed microphones ("bugs"). Now, however, technological developments have significantly expanded the range of electronic surveillance options. These include miniaturized transmitters for audio surveillance, lightweight compact television cameras for video surveillance, improved night vision cameras and viewing devices, and a rapidly growing array of computer-based surveillance techniques. In addition, most forms of electronic communication—whether via wire, coaxial cable, microwave, satellite, or even fiber optics—can be monitored if one has the time, money, and technical expertise. Encryption–the only technological countermeasure thought at this time to be generally effective—is still too expensive and cumbersome for widespread application, although costs are declining and ease of use is improving.

The primary purpose of electronic surveillance is to monitor the behavior of individuals, including individual movements, actions, communications, emotions, and/or various combinations thereof, as well as the movement of property or objects. Some uses of electronic surveillance devices may infringe on the protections afforded by the first, fourth, and fifth amendments to the U.S. Constitution and various public laws.

This chapter surveys the Federal Government's use of electronic surveillance and outlines a framework for the analysis of electronic surveillance issues.

Based on a review of available reports and the results of its Federal Agency Data Request, OTA found that:

- The extent of use of electronic surveillance by the private sector is unknown.
- The number of Federal and State court-approved wiretaps and bugs reported in 1984 was the highest since 1973.
- The number of Federal court-approved bugs and wiretaps in 1984 was the highest ever.
- According to early reports, an average of about 25 percent of intercepted communications in 1984 were reported to be incriminating in nature, with 2,393 persons arrested as a result of electronic surveillance.
- About 25 percent of Federal agency components responding to the OTA Federal Data Request indicated some use of electronic surveillance. [2]

[1] See Alan F. Westin, "Public and Group Attitudes Toward Information Policies and Boundaries for Criminal Justice," in U.S. Department of Justice, Bureau of Justice Statistics, *Information Policy and Crime Control Strategies,* Proceedings of a BJS/SEARCH Conference, July 1984, pp. 32-46; and William H. Dutton and Robert G. Meadow, "Public Perspectives on Government Information Technology: A Review of Survey Research on Privacy, Civil Liberties, and the Democratic Process," OTA contractor report, January 1985.

[2] Due to the unclassified focus of this study, two Department of Defense components—the National Security Agency and Defense Intelligence Agency-along with the Central Intelligence Agency were excluded from the data request.

53.548 O - 85 - 2 : QL 3

– Federal agency use is concentrated in components of the Departments of Justice, Treasury, Defense, Agriculture, and Interior.
— The Drug Enforcement Administration and Federal Bureau of Investigation (Justice), U.S. Customs Service (Treasury), and Air Force Office of Special Investigations (Defense) use the greatest number of different types of electronic surveillance technologies.
— The FBI, which currently uses nine different types of surveillance technologies, has plans to use eight additional types of technologies.

A thorough review of the technology and policy history of electronic surveillance led OTA to conclude that:

- The existing statutory framework and judicial interpretations thereof do not adequately cover new and emerging electronic surveillance technologies. Indeed, the courts have asked Congress for guidance on the new technologies.
- There is no immediate technological answer to protection against most electronic surveillance, although there are emerging techniques to protect communication systems from misuse or eavesdropping (e.g., low-cost data encryption).
- Despite a lack of coordination in electronic surveillance policymaking among the three branches of Government and the ad hoc nature of that policy, there are seven general components that are found in existing policies, be they legislative, executive, or judicial:
  1. a way of checking on the discretion of the Government agent in the field;
  2. a listing of the crimes and circumstances for which a particular type of electronic surveillance is considered appropriate;
  3. a standard to indicate at what stage in an investigation the use of a particular surveillance technique is appropriate;
  4. a justification for the need to use a particular surveillance technique;
  5. an account of how the scope of the surveillance will be minimized;
  6. a requirement to give notice after the fact to the subject of the surveillance; and
  7. remedies and sanctions, including a statutory exclusionary rule or a civil remedy.
- In setting electronic surveillance policy, Congress, the executive branch, and the courts, implicitly or explicitly, balance the societal interest in maintaining civil liberties protections for the individual against the societal interest in successful Government investigations. Based on an evaluation of previous policy formulation, policymakers, more or less consciously, have looked to certain dimensions in determining this balance.
- In determining the civil liberty interest with respect to electronic surveillance, policymakers look to five dimensions—the nature of information, the nature of the place or communication, the scope of the surveillance, the surreptitiousness of surveillance, and the pre-electronic analogy of the surveillance technique or device.
- In determining the Government's interest, policymakers have used three dimensions to evaluate the need for using an electronic surveillance technique or device-the purpose of the investigation, the degree of individualized suspicion, and the effectiveness of the electronic device as an investigatory tool compared to nonelectronic options.

This policy framework is applied in the following chapters to specific types of electronic surveillance technology.

INTRODUCTION

The capabilities for surveillance-the observation and monitoring of individual or group behavior including communication-are greatly expanded and enhanced with the use of technological devices. For example, technology makes it more efficient and less conspicuous to track movements, to hear conversations, to know the details of financial and other personal transactions, and to combine information from diverse sources into a composite file.

New surveillance tools are technically more difficult to detect, of higher reliability and sensitivity, speedier in processing time, less costly, more flexible and adaptable, and easier to conceal because of miniaturization and remote control. Current R&D will produce devices with increased surveillance capabilities, e.g., computer speech recognition and speaker identification, fiber optics, and expert systems.

Many electronic devices are currently available for monitoring individual or group behavior. For example, phone conversations might be overheard, records of phone numbers dialed might be accessed, movements at home and in the workplace might be video-recorded, and movements outside the home or workplace, even in the dark, could be observed. In addition, bank and credit records could be examined electronically to determine financial habits and general movements, and conversations in a public place could be recorded by a parabolic microphone. Further, it is possible that actions might be evaluated by computer to determine whether they match any profiles or have a pattern, that electronic mail communication might be accessed and read, that the movements of physical objects such as a car might be tracked by a beeper, and that a new friend or local taxi driver might be wired for sound.

From a law enforcement and investigative standpoint, the potential benefits offered through new electronic technologies may be substantial-e. g., the development of more accurate and complete information on suspects, the possible reduction in time and manpower required for case investigation, and the expansion of the options for preventing and deterring crimes. From a societal perspective, the possible benefits are also important–including the potential to increase one's sense of physical security in the home and on the streets, improve the capability to know when someone is in need of assistance, strengthen efforts to prevent the sale of illegal substances, and enhance the protection of citizens and Government officials from terrorist actions.

However, while providing increased security, the use of sophisticated technologies for surveillance purposes also presents possible dangers to society.[1] Over time, the cumulative effect of widespread surveillance for law enforcement, intelligence, or other investigatory purposes could change the climate and fabric of society in fundamental ways. For example, how will hotlines that encourage people to anonymously report potentially damaging information and one-party consent to the monitoring of conversations affect the level of trust in our society? Will private space and anonymity be preserved when individuals increasingly must make private information widely available, e.g., to banks, medical clinics, and credit agencies, in order to carry on everyday activities? How will informality and spontaneity in communications and behavior be affected as more personal activities are "on the record' or "in view?"

But most importantly for the purposes of this study, the use of electronic surveillance devices may infringe on the protections afforded in the first amendment (freedom of speech and press, and the right to peaceably assemble and to petition the Government for a redress of grievances), fourth amendment (unreasonable searches and seizures), and fifth amendment (protection against self-incrimination). The use of such devices may also conflict with procedural and substantive protections in specific statutes, e.g., Title III of the

[1]Gary T. Marx, "The New Surveillance," *Technology Review*, vol. 88, No. 4, May June 1985, pp. 42-48.

1968 Omnibus Crime Control and Safe Streets Act, the Privacy Act of 1974, the Foreign Intelligence Surveillance Act of 1978, the Electronic Funds Transfer Act of 1978, and the Cable Communications Policy Act of 1984.

Many innovations in electronic surveillance technology have outstripped constitutional and statutory protections, leaving areas in which there is currently no legal protection against, or controls on the use of, new surveillance devices. In 1928, Justice Louis Brandeis, in his dissenting opinion in Olmstead v. *United States,* warned that:

> Subtler and more far reaching means of invading privacy have become available to the Government . . . the progress of science in furnishing the Government with means of espionage is not likely to stop with wiretapping. Ways may some day be developed by which the Government. without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home.[4]

Although use of some surveillance techniques requires a court order, many do not require any authorized approval and some are not even covered by judicial interpretation of the fourth amendment prohibition on unreasonable searches and seizures. Additionally, the privacy and procedural rights of those subject to surveillance may also be violated, since their activities may be monitored even though no criminal suspicion has attached to them. Finally, given the unobtrusive nature of surveillance activities, it may be difficult to detect when one's rights have been violated.

The use of electronic surveillance devices may result in more efficient law enforcement. Their use may be required in part by the use of more evasive and sophisticated devices by those suspected of engaging in criminal activities. Yet, the cumulative impact of the increased use of surveillance, with or without a court order, is an important consideration for any society that prides itself on limited government and individual freedom.

The key policy issue is to determine the appropriate balance between the civil liberty interests and the intelligence, law enforcement, or other governmental interests involved. In some circumstances, the law enforcement interest will be great enough to outweigh the civil liberty interest. In other circumstances, the reverse will be the case. Policy, be it judicial, legislative, or administrative, seeks to define the parameters for this balancing process.

James Madison addressed this basic dilemma of democratic governments in *Federalist #51:*

> If men were angels, no government would be necessary. If angels were to govern men, neither external nor internal controls on government would be necessary. In framing a government which is to be administered by men over men, the great difficulty lies in this: You must first enable the Government to control the governed; and in the next place, oblige it to control itself.

[4] *Olmstead v. United States,* 277 U.S. **438, 473-474** (1928).

BACKGROUND

Technology and Use

For much of the 20th century, electronic surveillance technology was limited primarily to audio surveillance devices such as telephone taps and concealed microphones ("bugs"). In the late 1960s, however, technological developments began to significantly expand the range of electronic surveillance options. These included miniaturized transmitters for audio surveillance, lightweight compact television cameras for video surveillance, improved night vision cameras and viewing devices, and the first computer-based surveillance techniques. In the 1970s, congressional attention focused on electronic surveillance, partly due to the use of surveillance technologies during the Civil Rights Movement and in Watergate, but also

due to a perception of a growing application of such technology in various sectors of society. Table 1 presents a list of categories and types of surveillance technology as developed by the Subcommittee on Constitutional Rights of the Senate Committee on the Judiciary in 1976.

The primary purpose of electronic surveillance technology is to monitor the behavior of individuals. As illustrated in table 2, electronic devices can be used to monitor individual movements, actions, communications, emotions, and/or various combinations thereof.

It appears that many of the electronic surveillance technologies identified in table 1 were not widely used in 1976, partly because the underlying media of communication (e.g., electronic mail and cellular radio) were not in wide service. However, there is no authoritative information on the full extent of their use.

Table 1 .–Categories of Surveillance Technology

1. Electronic *eavesdropping technology* (audio survei l lance)
   - . radiating devices and receivers (e g , miniaturized transmitters)
   - . nonradiating devices (e g., wired surveillance systems, Including telephone taps and concealed microphones)
   - • tape recorders
2. Optical/imaging technology (visual surveillance)
   - • photographic techniques
   - • television (closed circuit and cable)
   - . night vision devices (use image intensifier to view objects under low light)
   - • satellite based
3. Computers and *re/ated technologies* (data surveillance)
   - • microcomputers —decentralization of machines and distributed processing
   - Ž computer networks
   - • software (e. g., expert systems)
   - • pattern recognition systems
4. *Sensor technology*
   - • magnetic sensors
   - • seismic sensors
   - . ınfrared sensors
   - • strain sensors
   - • electromagnetic sensors
5. Other devices and technologies
   - • citizen band radios
   - . vehicle location systems
   - • machine-readable magnetic strips
   - •s polygraph
   - • voice stress analyzer
   - • voice recognition
   - • laser interception
   - Ž cellular radio

SOURCE Based on the framework developed by the Senate Judiciary Committee s Subcommittee on Constitut ıon al Rıg hts ınits report *Surveillance Technology – 1976* seepp 29 37)

Table 2.—Categories of Behavior Subject to Electronic Surveillance

1. Movements—where someone Is. Individuals can be tracked electronically via beepers as well as by monitoring computerized transactional accounts in real time
2. Actions-what someone is doing or has done. Electronic devices to monitor action include: monitoring of keystrokes o n computer terminals, monitoring of telephone numbers called with pen registers, cable TV monitoring, monitoring of financial and commercial computerized accounts. and accessing computerlzed law enforcement or investlgatory systems.
3. Communications—what someone is saying or writing. and hearing or receiving. Two-way electronic communications can be intercepted whether the means be analog or digi - tal communication via wired telephones, communication via cordless or cellular phones, or digital electronic mail communication. Two-way nonelectronic communication can be intercepted via a variety of m microphone devices and other transmitters.
4. *Actions* and communications —the details of what some one is doing or saying Electronic visual surveillance, generally accompanied by audio surveillance, can monitor the actions and communications of individuals i n both private and public places, in daylight or darkness
5. Emotions —the psychological and physiological reactions to circumstances. Polygraph testing, voice stress analyzers, breath analyzers, and brain wave analyzers attempt to determine an Individual's reactions.

SOURCE Offi ce of Technology Assessn ent

In the private sector (not involving the Government), the FBI notes that the number of reported incidents of illegal interception of private sector communications declined from 524 in 1981 to 392 in 1984.[5] However, it is likely that only a small fraction of total incidents occurring are reported, and it is probable that many forms of private sector electronic surveillance go undetected, and if detected, go unreported.

Statistics on Government use of some electronic surveillance techniques, primarily telephone wiretaps and hidden microphones, are collected and published by the Administrative Office of the U.S. Courts. The April 1985 report indicates that in 1984, Federal and State judges approved 801 out of 802 requests for electronic surveillance-289 by Federal judges

[5] John Horgan, "Thwarting the Information Thieves," *IEEE Spectrum*, July 1985, p. 32, which cites the source as FBI spokesperson William Carter.

and 512 by State judges. The 1984 combined total of 801 was the highest since 1973. The 1984 Federal total of 289 was the highest ever, with the prior peak year being 1971. Overall, the number of State electronic surveillance orders has slowly declined since 1973, while Federal surveillance orders declined from 1971 to 1977, remained about constant from 1977 to 1980, and increased from 1981 to the present. The number of electronic interceptions authorized by Federal courts in 1984 is almost triple the 1981 level.[6]

In general, the reported electronic surveillance is used primarily in narcotics and gambling cases; in 1974 gambling was first and narcotics second, and in 1984 the order was reversed. The reported cost of electronic surveillance has increased dramatically, from about $8,000 each in 1974 to about $45,000 each in 1984. An average of about 25 percent of intercepted communications in 1984 was reported to be incriminating in nature, with 2,393 persons arrested as a result of electronic surveillance and about 27 percent of those convicted.[7] The figures for arrests and convictions are necessarily incomplete because of the time involved in concluding a Federal criminal case.

Because of the general lack of information on Federal use of electronic surveillance, questions on this topic were included in the OTA Federal Agency Data Request sent to the 13 cabinet-level departments and 20 selected independent agencies. Of 142 agency components responding, 35 or about 25 percent reported some current use of electronic surveillance technology for monitoring the movement, activity, conversation, or information pertaining to individuals or agencies in which the agency has an investigative, law enforcement, and/or intelligence interest. Of these 35 agency components, the top 15 agencies reporting use of the largest number of electronic surveillance technologies are listed in table 3. (Note that the Central Intelligence Agency, National Security Agency, and Defense Intelligence Agency were excluded from the data request.)

Table 3.—Top Fifteen Agency Components Using Electronic Surveillance Technology

Agency[a]	Number of technologies currently used
Drug Enforcement Administration (DOJ)	10
Federal Bureau of Investigation (DOJ)	9
U.S. Customs Service (Treasury)	9
U.S. Air Force (DOD)	9
National Park Service (DOI)	8
Internal Revenue Service (Treasury)	7
Criminal Division (DOJ)	7
U.S. Forest Service (USDA)	7
Inspector General (USDA)	7
Agricultural Stabilization and Conservation Service (USDA)	7
U.S. Army (DOD)	6
Fish and Wildlife Service (DOI)	6
U.S. Marshals Service (DOJ)	6
U.S. Mint (Treasury)	6
Bureau of Alcohol, Tobacco and Firearms (Treasury)	6

[a]The Central Intelligence Agency National Security Agency, and Defense Intelligence Agency were excluded due to the unclassified focus of this study

SOURCE Office of Technology Assessment

Use of specific technologies varied widely, with use of closed circuit television, night vision systems, radio scanners, and miniature transmitters indicated by many agencies that conduct electronic surveillance, and use of telephone taps, vehicle location systems (e.g., beepers), sensors, and pen registers indicated by a smaller but still significant number of agencies. The other technologies are used by relatively few or very few agencies. Actual results of the OTA Data Request are summarized in table 4. Out of the 35 agencies indicating some electronic surveillance activity, the FBI and DOD Inspector General's Office indicated the largest planned expansion in use of electronic surveillance technologies (see table 5).

The technical literature suggests that most forms of electronic communication can be intercepted, although it may be difficult and costly. The cost of equipment needed to intercept microwave telephone circuits has been estimated at about $40,000, but it can be done relatively easily and without the awareness of

[6]Administrative Office of the United States Courts, *Report on Applications for Orders Authorizing or Approving the Interception of Wire or Oral Communications*, for Calendar 1984, Washington, DC, April 1985, pp. 3, 6, 21.

[7]Ibid., pp. 6, 7, 21.

Table4 .—Electronic Surveillance Technology: Current and Planned Agency Use

Technology	Number of agency components reporting: Current use	Planned use	Total
Closed circuit television	25	4	29
Night vision systems	21	1	22
Miniature transmitters	19	2	21
Radio receivers (scanners)	19	1	20
Vehicle location systems (e. g., electronic beepers)	13	2	15
Sensors (e. g., electromagnetic, electronic, acoustic)	12	3	15
Telephone taps and recorders	13	1	14
Pen registers	11	3	14
Telephone usage monitoring	7	3	10
Computer usage monitoring	4	2	6
Electronic mail monitoring or interception	1	5	6
Cellular radio interception	3	2	5
Pattern recognition systems	2	2	4
Satellite interception	1	3	4
Expert systems/artificial intelligence	0	3	3
Voice recognition	0	3	3
Satellite-based visual surveillance systems	1	1	2
Microwave interception	1	1	2
Fiber optic interception	0	1	1

SOURCE-Office of Technology Assessment

Table 5.—Agency Components Indicating the Largest Projected Use of Electronic Surveillance Technologies

Agency	Number of current plus planned technologies
Federal Bureau of Investigation (DOJ)	17
Office of the Inspector General (DOD),	13
Drug Enforcement Administration (DOJ)	11
U.S. Customs (Treasury)	10
U.S. Air Force (DOD)	9
National Park Service (DOI)	9
Internal Revenue Service (Treasury)	9
Office of the Inspector General (USDA)	9
Agricultural Stabilization and Conservation Service (USDA)	9

SOURCE Off Ice of Technology Assessment

the network owner. Some believe that even fiber optic circuits can be tapped (but with difficulty), although this technology is so new that reliable information is scarce. The major electronic countermeasures include radiation shielding of electronic equipment (to prevent eavesdropping of signals given off by such equipment), spread-spectrum transmission, and encryption. Many technical experts believe that encryption is the only sure way to "protect any form of electronic communications end-to-end. "[8 9]

Policy

The history of electronic surveillance policy significantly involves all three branches of Government: the judiciary, Congress, and the executive branch. Key activities and policy actions are highlighted below.

Judicial

The courts have had a significant role in interpreting the Constitution and various statutes as they apply to electronic surveillance.

Constitutional questions regarding the legitimacy of the use of electronic surveillance devices under specific circumstances most often turn on an interpretation of fourth amendment protections. The fourth amendment provides that:

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

The critical triggering phrase of the fourth amendment is "searches and seizures. " If there is no search or seizure, then official behavior is not covered by the fourth amend--ment, and it need not be reasonable, based on probable cause, or carried out pursuant to a warrant. Although there may be statutory protections that require certain conduct, an individual does not have fourth amendment protections unless there is a search and seizure. The secondary triggering phrase of the fourth amendment is "unreasonable." Even if official conduct is regarded as a search or seizure, there is no invasion of fourth amendment pro-

[8] Horgan, op. cit., pp. 30, 31, 33, 34, 38.

[9] For further discussion of technical vulnerabilities and related security measures, see the forthcoming OTA study on "New Communications Technology: Implications for Privacy and Security" expected to be published in winter 1986/87.

tections if the conduct is reasonable. Determination of reasonableness depends on the judicial balancing of the individual interest, generally regarded as a privacy interest, against the governmental interest, including law and order, national security, internal security, and the proper administration of the laws. Reasonableness generally entails a predicate of probable cause and, with many exceptions, the issuance of a warrant.

The meaning and scope of the fourth amendment have involved judicial construction of these key phrases. Definition of "searches" has come to be a crazy patchwork quilt, depending partly on whether the search involves a person's body or home, partly on how public the activity is, partly on the degree of invasion or intrusiveness involved in conducting the search, partly on the facts of the case under consideration, and partly on who is on the Court.[10]

Searches using some form of electronic monitoring at first posed difficult problems for the Court because the searches did not comport with traditional definitions of a search-they did not involve physical trespassing and were often conducted in a public place. Until 1967, electronic monitoring of conversations was not regarded as a search under the fourth amendment.[11] In the landmark case of Katz v. United States (1967), the Court ruled that wiretapping was a search under the fourth amendment. As is often the result of landmark cases, subsequent legal analysis and judicial construction have raised more questions than the case first resolved. This is especially true with respect to the two phrases most important for subsequent legal decisions–a "reasonable expectation of privacy" [12] and "the fourth amendment protects people, not places. "[13]

Following Katz, judicial determination of whether a "search or seizure' '-has occurred depends on whether or not the individual has a "reasonable expectation of privacy" in the area or activity under surveillance. In determining whether or not an individual has such an expectation, the Supreme Court has adopted as its test the two-part formulation from Justice Harlan's concurring opinion:

> . first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as "reasonable. " [14]

The subjective part of the test focuses attention on the means the individual employs to protect his or her privacy, e.g., closing the door of a phone booth or closing curtains. Additionally, the assumption of risk that the individual appears to take is considered in determining the individual's actual expectation of privacy. Under assumption of risk, an individual is presumed to assume the risk that another party to a conversation or activity may consent to a search. This assumption of risk prevails even if the consenting party is an informer or undercover agent. "

The objective part of the test looks to what society regards as a reasonable expectation of privacy. Yet, it requires this without specifying an objective referent. Is "society" today's opinion polls, longstanding norms and traditions, a reasonable person, or the knowledge that people have in common? The result of the objective part of the test is that the Court has implicitly constructed a continuum of circumstances under which society would regard an individual as having a reasonable expectation

[10] For summary of Supreme Court rulings see: Anthony G. Amsterdam, "Perspectives on the Fourth Amendment, " 58 *Minnesota Law Review 349 (1974);* and Peter Goldberger, "Consent, Expectation of Privacy, and the Meaning of 'Searches' in the Fourth Amendment, " 75 *The Journal of Criminal Law and Criminology' 319 (1984).*

[11] *See* app. 2A for summary of relevant Supreme Court opinions.

[12] *Katz v. United States,* 389 U.S. 347, 360 (1967).

[13] Id. at 351.

[14] Id. at 361.

[15] See the "false friends cases' '– United *States v. White,* 401 U.S. 745 (1971), *Hoffa v. United States, 385* U.S. 293 (1966), and *Lopez v. United States, 373* U.S. **427 (1967).** In *White* the Court ruled that agents can be wired for sound and still be covered by the assumption of risk, reasoning that the risk did not increase materially simply because the informers were transmitting the conversation electronically. See also: Eric F. Saunders, "Electronic Eavesdropping and the Right to Privacy, " 52 *Boston University Law Review 831 (1973). Smith v. Maryland, 442* U.S. 735 (1979) and *United States v. Knotts, 103 S.* Ct. 1081 (1983) suggest that an individual forfeits his expectation of privacy by risking the possibility that his activities will be revealed to the police.

of privacy. The continuum ranges from public places ("open fields," "in plain view," "public highway"), in which there is no objective expectation of privacy except in unusual circumstances, to the inside of one's home with the windows and curtains shut and the door bolted, in which there is an objective expectation of privacy. The objective expectation of privacy along the continuum (shopping centers, motels, offices, automobiles, and yards) depends on judicial interpretation. Recently, the Court has modified the objective element, referring to it as a "legitimate' expectation of privacy."

The second important component of Katz is the holding that "the fourth amendment protects people, not places." The question of what protection the fourth amendment offers people remains unanswered, and defining the scope of such protection still necessitates reference to places. Moreover, the distinction between "people" and "places" has raised the question of whether the fourth amendment still protects property interests, or whether it now protects only more personal interests. The issue of the protection afforded people as distinct from that afforded places has become more significant with the growth of third-party recordkeepers, e.g., banks. The thrust of the Court opinion in Katz seemed to represent an expansion, not a replacement, of the existing fourth amendment protections:

> The amendment protects individual privacy against certain kinds of governmental intrusion, but its protections go further, and often have nothing to do with privacy at all.[17]

[16] First used by Justice Powell in *Couch v United States*, 409 U.S. 322 (1973) in rejecting a fourth amendment objection to an IRS summons and later used by Powell in *United States v. Miller*, 425 U.S. 435 (1976). In *Rakas v. Illinois*, 439 [J. S. 128 (1978), Justice Rehnquist referred to expectations of privacy "which the law recognizes as 'legitimate,'" This modification gives the objective part of the test a positive law, rather than societal expectation, meaning. This has practical as well as theoretical importance in that the courts would not ask whether society would regard an expectation of privacy in a particular case as reasonable, but would instead examine the laws to determine expectation. Although this would require less subjective analysis by the courts, it seems to assume that the laws are correct and need not be evaluated against fundamental law, i, e., the fourth amendment. See Goldberger, op. cit., and Gerald G. Ashdown. "The Fourth Amendment and the 'Legitimate Expectation of Privacy,'" 34 *Vanderbilt law Review* 1289 (1981).

[17] *Katz v. United States*, 389 [J. S. 347, 350 (1967).

It has been argued that, based on Katz, analysis of privacy interests should replace the more traditional property analysis when the Government uses nonphysical methods of search and where relevant privacy interests do not have physical characteristics. The property aspect is viewed as still important because it gives specificity and concreteness to fourth amendment analysis.[18] Yet, in some recent rulings the Court has treated privacy as the only interest protected by the fourth amendment.[19] This implies a further narrowing of fourth amendment protection, both because property interests are not considered and because of the problems of defining privacy. As one legal commentator, concerned with the influx of new surveillance devices, noted:

> Confusion over the fourth amendment status of the beeper is unavoidable so long as privacy remains the central theoretical focus of fourth amendment analysis. Privacy, like most concepts of fundamental value, is a relative, indeterminate concept that is not *easily* converted into a workable legal standard.[20]

In evaluating the appropriateness of the use of electronic surveillance technologies by Government officials, the courts have worked within the framework established by *Katz*. *By analogy* to traditional surveillance devices, the courts have attempted to determine whether or not individuals have a "reasonable expectation of privacy." This becomes more difficult as surveillance devices become more technologically sophisticated because the analogy is often more remote and hence less convincing. The courts have generally continued to consider the place in which a surveillance device is located or the place that a device is monitoring. The courts generally have adopted the more expansive interpretation of Katz and have not abandoned higher levels of protection for certain places, e.g., homes and yards.

Yet, the Katz framework has not offered the courts sufficient policy guidance to deal with the range and uses of new surveillance tech-

[18] Note, "'Tracking *Katz*: Beepers, Privacy and the Fourth Amendment," 86 *Yale Law Journal*, pp 1461, 1479-80 (1977).

[19] Ashdown, op. cit., p. 1321.

[20] Note, *Yale Law Journal*, op. cit., p. 1477.

nologies. "Reasonable expectation of privacy" is an inherently nebulous phrase and, despite 20 years of judicial application, predicting its meaning in a new context is difficult. Determining whether a place is sufficiently private to offer protection against official surveillance is more and more difficult as the public sphere of activities encroaches on what was once deemed private.

Thus, the courts have, on several occasions, asked Congress to legislate in the area of electronic surveillance technology." Most *recently,* Judge Richard Posner, in a case involving the use of video surveillance, said:

> We would think it a very good thing if Congress responded to the issues discussed in this opinion by amending Title III [of the 1968 Omnibus Crime Control and Safe Streets Act] to bring television surveillance within its scope. [22]

Congressional [23]

Congress did not play an active or effective role in surveillance policy until 1968. Prior to that time, the only legislation affecting official use of surveillance technology was unintended. In 1934, Congress remodified the Radio Act of 1927 as the Communications Act. Section 605 of the 1934 Act provided that "No person not being authorized by the sender shall intercept any communication and divulge . . . the contents. " There was no specific legislative history for this section and it appears that the 1934 bill was not intended to change existing law.[24] This was the interpretation until 1938 when the Supreme Court, in *Nardone v. United States,* 302 U.S. 379, ruled that Section 605 prohibited all telephone wiretapping, even when done by Federal Government officers. In response, bills passed both houses of Congress allowing wiretapping under certain circumstances and with certain procedural requirements. But the session ended before the conference committee could resolve a difference between the two bills-the House bill explicitly criminalized unauthorized official surveillance.[25]

Despite Congress's failure to overrule Nar*done* by legislation, wiretapping continued because the Justice Department construed Section 605 as not prohibiting wiretapping itself, but only the interception and subsequent divulgence outside the Federal establishment. Additionally, the President issued an Executive order to allow wiretapping for national security purposes.

In the immediate post-war period, numerous bills authorizing electronic surveillance were introduced, but none was enacted into law. Starting in 1960, electronic surveillance became a major public issue and congressional activity became more focused and purposeful. The target was organized crime, a major priority of the Kennedy Administration.

The first major congressional action regarding surveillance was Title III of the Omnibus Crime Control and Safe Streets Act of 1968. Because it has served as a model for controlling Government surveillance, analysis of the statute is necessary.

The basic legislative history document, S. Rep. No. 1097, 90th Cong., 3d sess. (1968), describes the purpose of the statute as follows:

> ITlhe U.S. Supreme Court, on June 12,1967, handed down the decision in *Berger v. New York,* 388 U.S. 41, which declared unconstitutional the New York State statute authorizing electronic eavesdropping (bugging) by law enforcement officers in investigating certain types of crimes. The Court held that the New York statute, on its face, failed to meet certain constitutional standards. In the course of the opinion, the Court delineated the constitutional criteria that electronic surveillance legislation should contain. Title III was drafted to meet these standards and to conform with *Katz v. United States,* 389 U.S. 347 (1967).

---

[21] See, for example, *United States v. U.S. District Court (Keith), 407* U.S. 297 (1972) in which the court suggested that Congress should devise a scheme for foreign intelligence.

[22] *United States v. Torres,* No. 84-1077, p. 19 (7th Cir., Dec. 19, 1984).

[23] Material in this section is derived in large part from Herman Schwartz, "Surveillance: Historical Policy Review, " OTA contractor paper, March 1985.

[24] See: S. Rep. No. 781, 73 Cong., 2d sess. 11 (1934).

[25] See: S. Rep. No. 1790, 75th Cong., 3d sess. 3 (1983).

> Title 111 has as its dual purpose (1) protecting the privacy of wire and oral communications, and (2) delineating on a uniform basis the circumstances and conditions under which the interception of wire and oral communications may be authorized. "

The problem the statute was designed to solve was seen as a combination of "tremendous scientific and technological developments that have taken place in the last century [that] have made possible today the widespread use and abuse of electronic surveillance techniques, and "a body of law [that] from the point of view of privacy or justice [i.e., law enforcement] is . . . totally unsatisfactory. "[27] The preamble to Title III reflects these aims: 1) to obtain evidence of "certain major types of offenses, and to cope with "organized criminals and 2) to safeguard the privacy of innocent persons and to provide "assurances that the interception is justified and that the information obtained thereby will not be misused.

In order to achieve these purposes, the statute provides that electronic surveillance of conversations is prohibited, upon pain of a substantial jail sentence and fine, except for: 1) law enforcement surveillance under a court order; 2) certain telephone company monitoring to ensure adequate services or to protect company property; 3) surveillance of a conversation where one participant consents to the surveillance; and 4) surveillance covered by the Foreign Intelligence Surveillance Act of 1978 (as Title 111 was later amended). I.aw enforcement surveillance must meet certain procedural requirements, which include:

1. an application for a court order approved by a high-ranking prosecutor (not by a policeman);
2. surveillance only for one of the crimes specified in Title III (the list was expanded in the early 1970s and again in October 1984 in the Comprehensive Crime Control Act);
3. probable cause to believe that a crime has occurred, the target of the surveillance is involved, and the evidence of that crime will be obtained by the surveillance;
4. a statement indicating that other investigative procedures are ineffective; and
5. an effort to minimize the interception.

A judge must pass on the application and may issue the order, and any extensions, if it meets the statutory requirements. Shortly after the surveillance ends, notice of the surveillance must be given to some or all of the people affected, as the judge decides, unless the judge agrees to postpone the notice. Illegally obtained evidence may not be used in any official proceedings, and a suit for damages may be brought for illegal surveillance, though a very strong good faith defense is allowed. In addition, the manufacture, distribution, possession, and advertising of devices for electronic surveillance for nonpublic use are prohibited.

There was little discussion of electronic surveillance by State officials during the legislative debates. Nevertheless, $2516(2) of Title III gives State officials wiretapping authority, if a State passes legislation modeled on the Federal act, for the investigation of:

> . . . murder, kidnapping, gambling, robbery, bribery, extortion, or dealing in narcotic drugs, marijuana or other dangerous drugs, or other crime dangerous to life, limb or property and punishable by imprisonment for more than one year . . . or any conspiracy to commit any of the foregoing offenses.

As of December 31, 1984, some 29 States and the District of Columbia have authorized their law enforcement officials to wiretap, though the State statutes differ in various ways.

On its face, Title III covers the interception of only conversations that are capable of be-

---

[26] Id. at 66. Three definitions in Title 11 I are important in determining the scope of the act:

1 *wire communication* means any communication made in w hole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of interstate or foreign commu nications,

2 *oral communication* me an> any oral communication uttered by a person exhibiting an expectation that such communication is not subject to Interception under circumstances justifying such expectation: and

3 *intercept* means the aural acquisition of the contents of any wire or oral communication through the use of any electronic, mechanical, or other device (Section 251() of Title 111)

[27] Id. at 67, 69.

ing heard by the human ear; data transmission, the video part of videotaping, pen registers, and other forms of communication are not covered. [28] The statute also permits interception for official purposes where one of the parties to the conversation has consented to the interception; private interceptions where one party consents are also exempt from the statutory ban unless the interception is for a criminal, "injurious," or tortious purpose. Evidence obtained in violation of the statute is excluded from all judicial or administrative proceedings, but only someone whose privacy was invaded can challenge the evidence.

The other major statute regulating the use of surveillance devices by Government officials is the Foreign Intelligence Surveillance Act of 1978 (FISA). This act establishes legal standards and procedures for the use of electronic surveillance in collecting foreign intelligence and counter-intelligence within the United States. This was the first legislative authorization for foreign intelligence wiretapping and other forms of electronic surveillance.'[8] The scope of this act is broader than Title III. FISA defines electronic surveillance broadly to include four categories: 1) *wiretaps,* including not only voice communications but also teleprinter, telegraph, facsimile, and digital communications; 2) *radio intercepts; 3) monitoring devices,* which may include microphone eavesdropping, surreptitious closed circuit television (CCTV) monitoring, transmitters that track movements of vehicles, and other techniques; and 4) *watch listing.* However, the application of FISA protection in the latter three categories is limited to those circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes. [30] The act created the Foreign Intelligence Surveillance Court, composed of seven Federal District Judges, to review and approve surveillance capable of monitoring U.S. persons (defined as U.S. citizens, lawfully admitted permanent resident aliens, and domestic organizations or corporations that are not openly acknowledged to be directed and controlled by foreign governments) in the United States. The procedural requirements of FISA apply only to electronic surveillance for foreign intelligence purposes, but the criminal penalties appear to apply more broadly to include law enforcement surveillance.[31]

There are a number of other statutes that place controls on the procedures and techniques of Government surveillance depending on the type of information that is being sought, e.g., the Privacy Act of 1974, the Right to Financial Privacy Act of 1978, the Electronic Funds Transfer Act of 1980, the Privacy Protection Act of 1980, and the Cable Communications Policy Act of 1984. (See appendix 2B for a summary of these statutes.)

Executive

Because of ambiguities in existing laws, executive officials have issued orders and guidelines to clarify the application of specific statutes or protections under particular circumstances or with respect to certain technological devices. Clarification of the scope and intent of FISA can be found in a number of Executive orders.[32]

In the absence of statutory or judicial guidance in the use of electronic surveillance for law enforcement and intelligence purposes, the Department of Justice (DOJ) generally issues policy guidelines that are regarded as requirements on agents of DOJ bureaus (FBI, Immigration and Naturalization Service, and Drug Enforcement Administration), and are usually considered as advisory by other agencies engaged in surveillance activities (e.g., Customs, Bureau of Alcohol, Tobacco and Firearms, IRS). For example, DOJ has issued policy guidelines for the use of electronic

[28] See S. Rep. No. 1097 at 90 (pen registers, etc., not included).
[29] See S. Rep. No, 98-660, "The Foreign Intelligence Surveillance Act of 1978: The First Five Years, " p. 1.
[30] Id. at 4.
[31] See Mar. 9, 1984 letter from John Keeney of the U.S. Department of Justice to U.S. Senator Patrick Leahy.
[32] See, e.g., Executive Order No. 12036, "United States Intelligence Activities, " Jan. 24, 1978 and updated as Executive Order No. 12333 on Dec. 4, 1981; also Executive Order No. 12139, "Exercise of Certain Authority Regarding Electronic Surveillance, " May 23, 1979.

visual surveillance and the use of pen registers. Such guidelines are issued to ensure that there are adequate procedural and substantive protections for individuals who are subject to surveillance, and that, therefore, information that is gathered through such surveillance will not be excluded as evidence in court,

FINDINGS AND POLICY IMPLICATIONS

1. The existing statutory framework and judicial interpretations thereof do not adequately cover new electronic surveillance technologies. Indeed, some courts have asked Congress for guidance on the new technologies,

See preceding discussion of policy history and background.

2. Despite a lack of coordination in electronic surveillance policymaking among the three branches of Government and the ad hoc nature of that policy, there are seven general components that are found in existing policies, be they legislative, executive, or judicial. Although the specifics of these components will vary given the different types of electronic surveillance being used, the general model is the same.

The first component of surveillance policies is a way of checking on the discretion of the Government agent in the field over whether to institute such surveillance. This can range from a field supervisor's approval to department-level approval to a U.S. Attorney's approval to a judicial warrant. The critical distinction in terms of level of approval necessary is whether the executive branch agency is responsible for authorizing the electronic surveillance or whether judicial approval is also necessary. In terms of checking agent discretion, judicial approval obviously represents a higher standard.

The second component is a listing of the crimes or circumstances for which a particular type of electronic surveillance is considered appropriate. Title 111 is a good example of this, as is the Foreign Intelligence Surveillance Act. In some situations, the list maybe quite broad but the principle remains. Crimes are categorized as misdemeanors and felonies with classes within each group. Electronic surveillance is generally only used for investigations of major felonies. Circumstances are often defined in terms of the governmental interest in pursuing the investigation. There is an implicit ranking of the importance of governmental interests for which surveillance devices are employed—national security, domestic security, law enforcement, and the proper administration of Government programs.

The third component of surveillance policies is some standard to indicate the degree of confidence about alleged criminal behavior that is necessary before the use of a particular surveillance technique is appropriate. This involves a showing of the evidence that has been accumulated to date, and a showing that the target of surveillance will provide additional evidence. The standard may range from probable cause, to reasonable suspicion, to reason to believe, to no need for any showing of evidence.

The fourth component is some justification for the need to use a particular surveillance technique or device. Generally, this requires a showing that more traditional forms of surveillance have failed, and some explanation as to how the surveillance technique under discussion will secure the necessary information.

The fifth component of surveillance policies is a requirement for an account of how the scope of the surveillance will be minimized to the particular party or parties under investigation and to those activities that seem criminally related.

The sixth component is the requirement that the individual be given some notice after the fact that he or she has been subject to surveillance, except in circumstances where notice would jeopardize an investigation or national security interests. There is no provision for notice in FISA, unless the party is being prosecuted.

The seventh component is a statement of the sanctions that apply if evidence is not collected in conformity with the requirements of the statute. An example of this is the exclusionary rule. Additionally, some statutes contain penalties for investigative agents who violate the statute, thus providing the individual with a civil remedy.

3. In applying the major components of electronic surveillance policy, the legislature, executive agency, or court, implicitly or explicitly, uses a framework for analysis. This framework involves balancing the societal interest in maintaining civil liberties protections for the individual against the societal interest in successful Government investigations. Based on an evaluation of previous policy formulation, it appears that policy makers, more or less consciously, have looked at certain dimensions in determining this balance.

Table 6 outlines the dimensions of the civil liberty interest v. the Government investigative interest found in existing electronic surveillance policy.

The dimensions of a civil liberty interest provide, to some extent, indicators for a "reasonable expectation of privacy" (Katz test) and the level of intrusiveness of the surveillance technology. In general, the more intrusive the technology, the more it violates "expectations of privacy' and the greater the threat to civil liberties. This has been an accepted principle since surveillance technologies were first used. Prior to Katz, the fourth amendment was interpreted to mean that "unreasonable" searches required physical intrusion into a constitutionally protected area. Following *Katz,* the physical trespass requirement was dropped. The Court has implicitly, if not often explicitly, continued to consider the intrusiveness of a search in determining its reasonableness, but intrusion is more broadly construed to go beyond mere physical trespass.

The difficulty in using intrusiveness as a principle by which to evaluate an "expectation of privacy" and the appropriateness of using a particular surveillance device is that no criteria have yet been explicitly formulated to determine intrusiveness. Instead, the facts of individual cases seem to be determinative. Yet, based on court rulings, congressional statutes, and executive orders, it is possible to isolate five dimensions that are important in determining the level of intrusiveness and the civil liberties interest that warrants protection.

Table 6.—Dimensions for Balancing Civil Liberty Interest v. Government Investigative Interest

Civil liberty *interest:*

1. *Nature of information:* The more personal or intimate the information that is to be gathered about a target, the more intrusive the surveillance technique and the greater the threat to civil liberties.
2. *Nature of p/ace communication.'* The more "private" the area or type of communication to be placed under surveillance, the more intrusive the surveillance and the greater the threat to civil liberties
3. *Scope of surveillance:* The more people and activities that are subject to surveillance, the more intrusive the surveillance and the greater the threat to civil liberties.
4. Surreptitiousness *of surveillance.'* The less likely it is for the individual to be aware of the surveillance and the harder it is for the individual to detect it, the greater the threat to civil liberties.
5. *Pre-electronlc analogy:* Pre-electronic analogies are often considered in determining ıntrusivenes[s], but with widely varying interpretations.

Government investigative intersert:

1 *Purpose of investigation:* Importance ranked as follows: national security, domestic security, law enforcement, and the proper administration of Government programs,
2. *Degree of individualized suspicion.* The lower the level of suspicion, the harder it is to justify the use of surveillance devices.
3, *Relative effectiveness:* More traditional Investigative techniques should be used and proven ineffective before using technologically sophisticated techniques.

SOURCE Off Ice of Technology Assessment

The first dimension is the nature of the information (content) that can be acquired. The more personal or intimate the information that is gathered, the more intrusive the surveillance technique and the greater the threat to civil liberties. Although ambiguous or incomplete information poses a threat to civil liberties, a surveillance technique that gathers more detailed information is generally regarded as more intrusive than one that gathers less detailed information. As a way of evaluating the specificity of information, the categorization of types of behavior that may be subject to surveillance (and illustrative surveillance technologies) may be useful (see table 2). Under this scheme, a surveillance technique that gathers information on movements would be

regarded as less intrusive than one that gathers information on actions and communication.

The second dimension is the "public" or "private" nature of the area (place) or communication to be placed under surveillance. The fourth amendment explicitly protects persons, houses, papers, and effects. The difficulty is that these can be more private or less private depending on where they are kept or who else is given access to them, Homes, phone conversations, and first class mail have traditionally been regarded as "private." In general, the more "private" the area or communication, the more intrusive the surveillance and the greater the threat to civil liberties.

The third dimension is the scope of the surveillance or the extent to which the surveillance covers persons not specifically under surveillance.[33] The importance of this principle is reflected in the minimization requirements of Title III and FISA. The broader the net cast, the more intrusive the surveillance and the greater the threat to civil liberties.

The fourth dimension is the surreptitiousness of the surveillance or the individual's ability to detect whether he or she is the target of surveillance. This ability to detect involves both the likelihood that the individual will be aware of the surveillance and also his or her ability to locate the source. This dimension is reflected in the concept of assumption of risk, which has been used as a justification for one-party consent to surveillance. It is also reflected in the lower standards for physical surveillance because it is assumed that an individual can easily monitor whether or not someone is following him or her. The harder it is for the individual' to detect the surveillance, the greater the threat to civil liberties.

The final factor that policymakers often consider in evaluating the civil liberty threat of an electronic surveillance device is the pre-electronic analogy of the surveillance technique. This focuses attention on a historical measure of privacy that provides a standard for preserving a certain level of privacy. Analogies are made to policy choices for a pre-electronic era. For example, what kinds of communications have traditionally been protected, i.e., first class mail and phone calls, and what modern communications are their counterparts? Two policy difficulties are presented by this factor. The first is that different people see different analogies. The second is that the intrusiveness of a pre-electronic device and its electronic counterpart is not always correspondent.

In evaluating the legitimacy of the Government's use of surveillance devices, three dimensions are considered. The first is the purpose of the investigation (the governmental interest). There is an implicit ranking of the importance of governmental interests for which investigations are carried out—national security, domestic security, law enforcement, and the proper administration of Government programs. The nature of the governmental interest determines the level of judicial or administrative control, both initially and at specified review stages. With respect to the use of electronic surveillance, the importance of the governmental interest is always considered, but is not determinative of the level of surveillance. The law enforcement interest is broadest, but most well developed in statute, e.g., Title III categories of crimes for which eavesdropping may be used. The national security and domestic security purposes have constitutionally allowed Government officials the greatest discretion in determining whether surveillance should be used. The rules for administrative searches are fairly well developed in statutes, but standards for the use of electronic surveillance often are not included.

The second dimension is the degree of individualized suspicion. In general, the earlier in the investigation the harder it is to justify the use of surveillance devices. This is so because it may be difficult to document that criminality is involved and that the target of

[33] See Donald L. Doerenberg, " 'The Right of the People': Reconciling Collective and Individual Interests Under the Fourth Amendment, " 58 *New York University Law Review 259 (1983),* who distinguishes the following possible targets of a search—all citizens, categories or classes of individuals, or a selected individual.

the surveillance is involved or can provide evidence. Traditionally, the standard for the Government's need to know varies depending on what it already knows. In theory, the more the Government knows, the less likely that it is engaging in a fishing expedition. If the Government has probable cause to believe that someone is implicated in a crime or terrorist activity, then it has a need to know more than if it had only a reasonable suspicion or reason to believe that someone was involved.

The third dimension is the relative effectiveness of electronic surveillance compared to other means that are available to secure the same information. In existing policies, the assumption is that there should be a demonstration that more traditional investigative techniques have been used and proven ineffective before using technologically sophisticated electronic techniques. An analysis of the effectiveness of the surveillance technology or device is important in determining the legitimacy of its use. If more accurate and complete evidence can be gathered through the use of an electronic surveillance device than through pre-electronic means, then serious consideration will be given to its use.

The following chapters describe a number of new electronic surveillance devices and techniques that have been made possible by technological advances and analyze their policy implications using the framework developed in this chapter.

APPENDIX 2A: KEY SUPREME COURT DECISIONS ON ELECTRONIC SURVEILLANCE

Olmstead v. United States, 277 U.S. 438 (1928)—a 5-4 decision ruling that neither the fourth nor fifth amendments to the Constitution applied to wiretapping. The fourth amendment did not apply because: there was no trespass; its protection is limited to material effects, not to intangibles like speech; and there was no protection for voice communication projected outside the house. The fifth amendment did not apply because there was no evidence of compulsion to talk over the phone and because the fourth was not first violated. Brandeis argued in his dissent that the fourth amendment protected a right to privacy, and stated:

> Moreover, "in the application of a Constitution, our contemplation cannot be only of what has been, but of what may be." The progress of science in furnishing the Government with means of espionage is not likely to stop with wiretapping. Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home. Advances in the psychic and related science may bring means of exploring unexpressed beliefs, thoughts and emotions. . . Can it be that the Constitution affords no protection against such invasions of individual security?

Public reaction to the decision was negative; bills were introduced in Congress, but none passed.

Nardone v. United States, 302 U.S. 379 (1937)–Court ruled that Section 605 prohibited telephone wiretapping by anyone, including Federal Government officers. Decision was criticized as "judicial legislation." Bills were introduced in Congress to allow wiretapping under certain circumstances, but none passed. Evidence indicates that wiretapping continued at the time despite decision.

Berger v. New York, 388 U.S. 41 (1967)–Court declared the New York wiretapping statute unconstitutional because it was not particular enough in describing the crime, or "the place to be searched," or the "persons or things to be seized" as specifically required by the fourth amendment.

Katz v. United States, 389 U.S. 347 (1967)–Court overruled *Olmstead,* thus bringing wiretapping under the fourth amendment. The Court developed a general formula to determine whether an investigative technique conflicts with the fourth amendment–does the individual evidence an expectation of privacy and is the expectation of privacy "one that society is prepared to recognize as 'reasonable?' " The Court's criteria for valid surveillance involved a warrant, particularization and probable cause requirements for suspect, crime, phone, and time.

United States v. U.S. District Court for the Eastern District of Michigan, 407 U.S. 297 (1972)–Court prohibited unauthorized electronic surveil-

lance to gather intelligence for domestic security purposes, holding that:

> . . . prior judicial approval is required for the type of domestic security surveillance involved in this case and that such approval may be made in accordance with such reasonable standards as the Congress may prescribe.

United States v. Miller, 425 U.S. 435 (1976)–Court ruled that a bank customer's financial record is the property of the bank, and thus he or she has no legitimate "expectation of privacy" in these records.

United States v. New York Telephone Co., 434 U.S. 159 (1977)–Court held that to be covered by Title III, a communication must be capable of being overheard.

Smith v. Maryland, 442 U.S. 735 (1979)–Court held that the use of a pen register did not violate the fourth amendment.

United States v. Knotts, 103 S. Ct. 1081 (1983) –Court held that the *warrantless* monitoring of a beeper is not a search and seizure under the fourth amendment because there is no reasonable expectation of privacy as the movements tracked are public.

United States v. Karo, 104 S. Ct. 3296 (1984)–Court held that using a beeper to trail a container into a house and "to keep in touch with it inside the house" did violate the fourth amendment.

APPENDIX 2B: KEY STATUTES RELEVANT TO ELECTRONIC SURVEILLANCE

Section 605 *of the Communications Act of 1934* provided that "No person not being authorized by the sender shall intercept any communication and divulge . . . the contents . . ."

Title III of the 1968 Omnibus Crime Control and Safe Streets Act is designed to protect the privacy of wire and oral communications and also to allow evidence to be obtained for "certain types of major offenses. " Law enforcement electronic surveillance of conversations is thus prohibited except under a court order, which a judge may issue after being convinced that the following procedural requirements have been met:

1. application by a high-ranking prosecutor;
2. surveillance for one of the crimes specified in Title III;
3. probable cause to believe that a crime has occurred, that the target of the surveillance is involved, and that the evidence of that crime will be obtained by the surveillance;
4. a statement indicating that other investigative procedures are ineffective; and
5. an effort to minimize the interception.

Crime Control Act of 1973 requires-that State criminal justice information systems, developed with Federal funds, be protected by measures to ensure the privacy and security of information.

Privacy Act of 1974 requires agencies to comply with fair information practices in their handling of personal information, including the following: records must be necessary, lawful, current, and accurate; records must be used only for purpose collected except with an individual's consent or where exempted; no record of an individual's exercise of first amendment rights is to be kept unless authorized by statute; information cannot be sold or rented for mailing list use. The following are exempted: CIA records; records maintained by law enforcement agencies; Secret Service records; Federal testing materials; etc.

*Foreign Intelligence Surveillance Act of 1978 es*tablishes legal standards and procedures for the use of electronic surveillance to collect foreign intelligence and counter-intelligence within the United States. This was the first legislative authorization for wiretapping and other forms of electronic surveillance (including radio intercepts, microphone eavesdropping, closed circuit television, beepers, and other monitoring techniques). It created the Foreign Intelligence Surveillance Court, composed of seven Federal District Judges, to review and approve surveillance capable of monitoring U.S. persons (defined as U.S. citizens, lawfully admitted permanent resident aliens, and domestic organizations or corporations that are not openly acknowledged to be directed and controlled by foreign governments) in the United States. The procedural requirements of FISA apply only to electronic surveillance for foreign intelligence purposes, but the criminal penalties appear to apply more broadly to include law enforcement surveillance.

Right to Financial Privacy Act of 1978 provides bank customers with some privacy regarding their

records held by banks and other financial institutions, and provides procedures whereby Federal agencies can gain access to such records.

Electronic Funds Transfer Act of 1980 provides that any institution providing EFT or other bank services must notify its customers about third-party access to customer accounts.

Privacy Protection Act of 1980 prohibits Government agents from conducting unannounced searches of press offices and files if no one in the press room is suspected of a crime.

Cable Communications Policy Act of 1984 requires the cable service to inform the subscriber of: the nature of personally identifiable information collected and the nature of the use of such information; the disclosures that may be made of such information; the period during which such information will be maintained; and the times during which an individual may access such information. Also places restrictions on the cable services' collection and disclosures of such information. The act creates a subscriber right to privacy against Government surveillance.