Chapter 3

Telephone Surveillance

Chapter 3
Telephone Surveillance

SUMMARY

The public generally expects that telephone conversations are private, and that electronic surveillance of telephone calls (sometimes known as wiretapping or eavesdropping) is illegal, except in very narrowly circumscribed law enforcement and national security investigations. But technological innovations now make it easier to electronically monitor both the content of phone calls and phone transactions (e.g., number called, time, and place called). Furthermore, the new telephone technology was not envisioned when current legal protections were enacted, and thus the statutory protection against telephone surveillance is weak, ambiguous, or nonexistent.

After reviewing and assessing relevant technological developments and the statutory framework, OTA found that:

- A host of new information technologies has revolutionized the telephone system since 1968—the last time Congress passed major legislation (Title III of the Omnibus Crime Control and Safe Streets Act) that covered telephone surveillance by law enforcement agencies and private parties.
- Significant new technologies include digital transmission (whereby many phone calls are converted from analog to digital form for transmission) and cellular and cordless phones, as well as the increased use of telephones for electronic transmission of data.
- Deregulation of the telephone industry, the proliferation of common carriers, and the growth of private (as opposed to common carrier) telephone companies also raise questions as to the applicability of existing legal protections for telephone privacy.
- The contents of phone conversations that are transmitted in digital form or made on cellular or cordless phones are *not* clearly protected by existing statutory and constitutional prohibitions on the interception of phone calls.
- Interception of the content of phone calls represents a substantial threat to civil liberties, but also a significant benefit to investigative authorities. This balancing is reflected in the standards and procedures presently embodied in Title III for such interception.
- New information technologies–e.g., advanced pen registers and automatic billing equipment—have also greatly increased the ability to collect and access transactional information about telephone calls (e.g., the numbers and places called).
- Transactional information is also *not* clearly protected under existing statutes and judicial precedents.

OTA identified three major options for congressional consideration with respect to policy on interception of the content of telephone calls:

- treat all calls similarly with respect to the extent of protection against unauthorized interception, i.e., extend Title III of the Omnibus Crime Control and Safe Streets Act to cover all phone calls-whether analog, digital, cellular, or cordless-and both voice and data communications;
- formulate special policies for specific telephone technologies; and
- do nothing and leave policymaking up to the development of case law depending on individual circumstances.

OTA also concluded that the deregulatory and market trends toward private telephone systems and hybrid common carrier-private systems indicate the need for congressional review of applicable provisions of the Commu-

nications Act of 1934 and Federal Communications Commission regulations, as well as Title III of the Omnibus Crime Control Act, with respect to telephone privacy protection.

Finally, OTA concluded that at present there is no feasible and cost-effective technological method to provide universal protection against telephone surveillance. A separate OTA study is examining future technical trends and safeguards against misuse as well as issues and options relevant to monitoring of transactional-as contrasted with content—information. *

*See the separate OTA study on "New Communications Technology: Implications for Privacy and Security," expected to be published in winter 1986/87.

INTRODUCTION

Most phone users have assumed a high degree of confidentiality for their phone calls. This has been especially true as private lines and improved connections replaced party lines and broken connections. In some respects, the technology has brought more assurances for the protection of the privacy of phone calls than did the law. However, this is now changing. Four technological innovations in phone service—digital transmission, new types of phones, new phone networks, and the ability to easily collect detailed information on phone usage—make it easier both to overhear the content of phone calls and also to monitor phone transactions. The law has not yet addressed these innovations, thus leaving gaps between the privacy that people expect and the privacy that they are assured.

With the conventional telephone, phone calls were transmitted in analog form across wire lines. Today, an increasing percentage of phone calls are converted from analog to digital form and then transmitted. Transmission may be over wire, but is often via microwave radio and satellite systems and, increasingly, via fiber optic transmission facilities. Statutes prohibiting wiretapping, primarily Title III of the Omnibus Crime Control and Safe Streets Act, were written to regulate the interception of oral communications transmitted in whole or in part by wire.

Additionally, new phones are making use, in whole or in part, of radio communications. Cellular or mobile phones use radio to transmit messages between a phone and a switching center, while cordless phones use radio to carry messages between the phone base station and the cordless phone handset. Section 605 of the 1934 Communications Act prohibits interception of radio communications. However, it does not protect phone calls because the courts have ruled that Congress intended Title III to be the exclusive remedy with respect to telephone interceptions.

Another growing gap in the protection afforded phone calls is between common carrier calls and private network calls. Legislation has addressed the former, while the latter have not been given any legal protection. Thus, the privacy of the content of digitized phone calls, cellular and cordless phone calls, and private carrier calls may not be afforded protection against interception by either Government officials or private parties.

Moreover, technological changes make it far easier today to monitor phone transactions. Pen registers are devices by which Government officials or private parties can monitor the numbers dialed on a given line. Presently, a court order is not necessary to install a pen register under Title III or the fourth amendment, but is required under the Foreign Intelligence Surveillance Act. Increasingly, computerized telecommunications switching equipment can collect and store information on the numbers dialed and length of phone calls. This information may be kept for billing and administrative purposes, but it also has monitoring capabilities. As automatic call accounting becomes widespread, pen registers will become unnecessary. A detailed historical record of long-distance and sometimes lo-

cal phone calls is now kept for perhaps 3 months by phone companies and can be accessed by Government officials with a subpoena. However, if a phone system is wholly or in part private, then this calling information is legally available to Government officials without a subpoena.

Before analyzing in detail the policy issues presented by these gaps in the protection for the content of phone calls and the record of phone transactions, a brief review of the history and background of technology and policy regarding wiretapping will be presented.

BACKGROUND[1]

Telegraph and telephone tapping by both private citizens and public officials began soon after the telegraph and telephone were invented. Some States tried to deal with telephone tapping either through their trespass statutes or by expanding early laws barring telegraph interceptions. However, the legality of Government surveillance under these statutes was usually unclear because there was no rule excluding illegally obtained evidence. By 1927, despite questions about the scope of coverage, some 28 States had made wiretapping a crime.[2]

Federal concern about wiretapping first surfaced in 1918 when the Federal Government began regulating the telephone system, but the concern was primarily for "the protection of the government and the property of the telephone and telegraph companies while under governmental control."[3] The Government barred tapping of, or interference with, telephone and telegraph messages, if the tap was done "without authority." This legislation expired in 1919. Civil liberties concerns first became important in the early 1920s, when wiretapping was used by the Department of Justice in its raids against aliens.[4] At this time, there were also reports that the phones and offices of members of Congress had been eavesdropped on.

In 1924, Attorney General Harlan Fiske Stone banned wiretapping by the Department of Justice, including the Bureau of Investigation (the FBI's predecessor). This effort at administrative control was only partially successful. The order bound only the Department of Justice and not the Treasury, which had jurisdiction over Prohibition enforcement, the law enforcement area that came to rely most on electronic surveillance. Prohibition agents continued to wiretap, even though the Treasury Department purported to be officially opposed to wiretapping.[5]

The Treasury's wiretapping ultimately brought the matter to the courts in *Olmstead v. United States, 277* U.S. 438 (1928). The Court, in a *5-4* opinion by Chief Justice Taft, ruled that neither the fourth nor fifth amendments to the Constitution provided protection against wiretapping.[6] The public reaction to the *Olmstead* decision was largely and strongly negative.[7] Immediately after *Olmstead* was decided, bills were proposed in Congress to ban wiretapping.[8]

[1] Material in this section is based in part on Herman Schwartz, "Surveillance: Historical Policy Review," contractor paper prepared for OTA, March 1985.

[2] See *amicus* brief for the telephone companies in *Olmstead v. United States,* **277** U.S. 438 (1928).

[3] H. R. Rep. No. 800, 65th Cong., 2d sess. (1918), reprinted in *Wiretapping, Eavesdropping and the Bill of Rights,* Hearings Before the Subcommittee on Constitutional Rights of the Senate Judiciary Committee, Part 4, Appendix to Part 3, 86th Cong., 1st sess. 792 (1959) ("1914-1959 Leg. Hist.").

[4] Alan Westin, *The Wire-tapping Problem,* 52 *Columbia Law Review 164, 172* n. 35 (1952).

[5] Walter F. Murphy, *Wiretapping on Trial: A Case Study in the Judicial Process (New* York: Random House, 1965), p. 13.

[6] The Court gave three reasons why the fourth amendment was not implicated: 1) officials had not trespassed onto *Olmstead* property; 2) the amendment did not apply to intangibles like speech, but only to material "effects"; and 3) there was no protection for voice communications projected outside the house, Justice Holmes wrote a short dissent, condemning the agents' conduct as "dirty business." Justice Brandeis wrote the main dissent in which he disagreed with the majority's reading of the precedents, its very narrow view of the fourth amendment, and its willingness to countenance criminal activity by the Government. **1914-59** Leg. Hist. **770-73.**

[7] Murphy, op. cit., p. 125.

[8] 1914-59 Leg. Hist. 881-83.

In 1934, Congress remodified the Radio Act of 1927, which was itself a recodification of legislation going back to 1912. 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.[9] Apparently no one thought Congress had taken an important step in dealing with electronic surveillance.

It thus came as a surprise to many when the Supreme Court in 1938 ruled that Section 605 prohibited all telephone wiretapping, even when done by Federal Government officers.[10] In 1957, the Court ruled that this applied to State officers as well.[11] The Nardone decision was generally criticized both in 1938 and later as "judicial legislation. "[12]

Congressional response to Nardone was swift, but did not result in legislation. This time, bills were introduced to allow wiretapping, provided that the head of a department believed a felony had been or was about to be committed by two or more people. Congressional concern about organized crime was one of the two primary reasons for authorizing electronic surveillance, the other being national security. Bills allowing wiretapping passed both houses, but the session ended before the conference committee could resolve a difference between the two bills-the House bill explicitly criminalized unauthorized official surveillance.[13] The ease with which both Houses passed bills allowing Federal surveillance might lead one to think legislation was imminent. But this did not happen, even though, despite the *Nardone* decision, the Federal Government and State officials continued to wiretap.[14]

During and after World War II, the FBI engaged in large amounts of electronic surveillance. Between 1940 and 1960, the FBI installed over 7,000 national security surveillances, with 519 taps and 186 bugs in 1945 alone; and the Treasury Department installed over 10,000 taps during 1934 to 1948. Other Federal agencies, like the military, also engaged in tapping and bugging. On the local level, the New York City police installed thousands of taps each year (e.g., 3,588 in 1953-54), mostly in morals and bookmaking investigations; studies by Samuel Dash and others have documented widespread tapping elsewhere.[15]

The tapping and bugging targeted many people who might not normally appear to be appropriate targets, a situation that continued at least into the 1960s. In 1941, for example, the Los Angeles Chamber of Commerce was tapped, on the authority of Attorney General Francis Biddle. Presidential aides and others were similarly tapped. The most complete information on these practices, as developed by the Church Committee, relates to FBI surveillances in the post-1960 period when Dr. Martin Luther King, Jr., Congressman Harold Cooley, journalists, and many others were put under electronic surveillance. [16]

At this time, questions were also being raised concerning the effectiveness of electronic surveillance and of judicial protections, as well as the persistent use of electronic surveillance in State law enforcement for minor crimes. [17] There was also much documentation

---

[9] See S. Rep. No. 781, 73d Cong., 2d sess. 11 (1934), reprinted in 1914-59 Leg. History 895; Report of the National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance 35 (1976).

[10] *Nardone v. United States,* 302 U.S. 379 (1937).

[11] *Benanti v. United States,* 355 U.S. 96 (1957).

[12] Report of the National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance, *Electronic Surveillance* (Washington, DC: NWC, 1976), p. 35.

[13] S. Rep. No. 1790, 75th Cong., 3d sess. 3 (1938), reprinted in 1914-59 Leg. Hist. 961; Murphy, op. cit., p. 135.

[14] See generally Samuel Dash, Richard F. Schwartz, and Robert E. Knowlton, *The Eavesdroppers (New* York: DeCapo, 1959).

[15] Ibid.; and Herman Schwartz, *Taps, Bugs, and Fooling the People (New* York: Field Foundation, 1977).

[16] See U.S. Congress, Senate Select Committee to Study Governmental Operations With Respect to Intelligence Activities, *Supplementary Detailed Reports on Intelligence Activities,* vol. III, 94th Cong., 2d sess. (Washington, DC: U.S. Government Printing Office, 1976).

[17] See Wiretapping Hearings before Subcommittee No. 5. U.S. House of Representatives Judiciary Committee, 84 Cong., 1st sess. 53, 67 (1955), ("1955 Hearings"), 194, 347, 359.

of illegal private wiretapping, by private detectives and others for industrial espionage and in domestic relations matters, and of the ineffectiveness of either Federal or State law to cope with this.

Competing pressures continued throughout the 1960s. The President's Commission on Law Enforcement and the Administration of Justice issued a report in 1967, and near the top of its priorities was organized crime. While it did not explicitly recommend the use of wiretapping, a majority of the Commission members did so. The American Bar Association proposed a statute that became the model for legislation permitting wiretapping that was ultimately enacted in 1968. Because of this activity, the arguments for wiretapping were repeatedly being made and given consideration. For example, Professor G. Robert Blakey, the chief draftsman of the ABA report and proposals and also of the 1968 Wiretap Act, told a congressional committee in 1967:

> The normal criminal situation deals with an incident, a murder, a rape, or a robbery, probably committed by one person. The criminal investigation normally moves from the known crime toward the unknown criminal. This is a sharp contrast to the type of procedures you must use in the investigation of organized crime. Here in many situations you have known criminals but unknown crimes.
>
> So it is necessary to subject the known criminals to surveillance, that is, to monitor their activities. It is necessary to identify their criminal and noncriminal associates; and their areas of operation, both legal and illegal. Strategic intelligence attempts to paint this broad, overall picture of the criminal's activities in order that an investigator can ultimately move in with a specific criminal investigation and prosecution. [18]

The pressures, however, were not all one-sided. In the mid-1960s, illegal tapping and bugging by the FBI, IRS, and others came to light when FBI bugs were accidentally discovered in a Las Vegas gambler's office and in Washington's Sheraton-Carlton Hotel and lawyer-client conversations were overheard. This led to a series of court-ordered revelations of illegal Federal surveillance involving some 50 or more cases. As a result, in 1965 President Lyndon B. Johnson ordered an end to all electronic surveillance except in national security cases. [19]

During this period, the Supreme Court overruled *Olmstead* in *Katz v. United States, 389* U.S. *347 (1967).* The *Katz* decision set out both a general formula for the interests protected by the fourth amendment and specific criteria for a statute authorizing law enforcement wiretapping. [20] The Court's specific criteria for a valid surveillance involved the conventional magistrate's warrant, and the equally conventional probable cause requirements applied to a specific telephone, for a specific need and crime, to the specific suspect conversations and the specific time during which he spoke. The Court also stressed that *prior* notice to the suspect of the interception was unnecessary, and indicated that notice after the interception was constitutionally acceptable. These requirements were drawn from previous related cases and from conventional fourth amendment principles.

All these factors, plus a growing concern about crime, came together to break the 30-year impasse since *Nardone* and produced Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §2500ff, which authorizes telephone tapping and microphone surveillance by Federal and State officials, if antecedent judicial approval is obtained. [21] Other than the Foreign Intelligence Surveillance Act in 1978, there has been no significant legislative action since that time, despite a virtual revolution in technology.

---

[18] Hearings on *Controlling Crime Through More Effective Law Enforcement* before the Subcommittee on Criminal Law and Procedures of the Senate Judiciary Committee, 90th Cong., 2d sess. 957-58 (196i'1,

[19] III Church Comm. 298-300.

[20] *Katz* expressly excluded national security surveillance from its discussion. See 389 U.S. at n. 21,

[21] See ch. **2** for a detailed analysis of the statute.

FINDINGS AND POLICY IMPLICATIONS

1. A host of new information technologies has revolutionized the telephone system since 1968—the last time Congress passed major legislation on telephone surveillance by law enforcement agencies and private parties. These technologies include digital transmission and cellular and cordless phones.

Each of the major technological developments affecting the telephone system is discussed briefly below.

Digital Transmission.—Initially, the phone system carried only analog signals over telephone wires. Much of the telephone system in the United States, and especially overseas, is heavily dependent on analog systems, at least for part of a phone call. Increasingly, however, analog voice signals are digitized. The phone system of the future will carry digitized information (voice, data, and image) across wires, optical fibers, microwave radios, and satellite links. The evolution of digital communications, as well as the digital switching devices that enable the system to function smoothly, is beginning to provide expanded services to customers.

The computing and telecommunications industries worldwide are gradually evolving toward a new system, the Integrated Services Digital Network (ISDN), which will allow the transmission of data, voice, image, and video over the same digital system worldwide. The future trend is toward a wholly digitized, efficient, and integrated phone system.[22] Some predict that, in the future, the microphones and speakers in the telephone handset will be the only analog components of the system.[23]

Legal or illegal interception and interpretation of digital signals is not significantly more difficult than for analog signals; the interceptor just needs a coder-decoder and knowledge of the modulation scheme. Digitization of phone calls, thus, does not offer more protection for the content of the call. Transmission over fiber optic lines may offer more protection against illegall interception, to the extent that the operating company can more easily tell when the line has been broken into and where along the line the break has occurred.[24]

Cellular Phones.–The cellular telephone is a technological innovation in providing quality mobile phone service to a large number of customers over an expansive geographic area. The basic technology was first developed at AT&T Bell Labs in the 1950s, and the necessary computer and switching technologies were developed in the 1960s. The critical development was a system that reused frequency spectrum by dividing a service area into "cells." Each cell contains a base station that serves as a radio transmit-receive-switching station. Cellular mobile phone calls are relayed by radio to the base station, which is hooked up to the mobile phone switching office computer. The switching office then routes calls to other base stations or to the telephone network via similar routes. If the call is to another cellular phone it is relayed to the appropriate cell site transmitter. If the party called is using a conventional wire-line phone, then the switching office computer routes it through the telephone system to the receiver.[25]

In 1982, the Federal Communications Commission (FCC) accepted applications for cellular license systems. It received 196 applications for the top 30 markets. The FCC decided to license two types of competitors, a tele-

[22] William Stallings, "The Integrated Services Digital Network," *Datamation*, Dec. 1, 1984, pp. 68-70.

[23] John G. Posa, "Phone Net Going Digital," *High Technology*, May 1983, p. 41.

[24] For trend in fiber optic systems, see Les C. Gunderson and Donald B. Keck, "optical Fibers: Where Light Outperforms Electronics," *Technology Review*, May/June 1983, pp. 33-44; Soichi Kobayashi and Tatsuya Kirnura, "Semiconductor Optical Amplifiers," *IEEE Spectrum*, May 1984, pp. 26-33; Jeff Hecht, "Outlook Brightens for Semiconductor Lasers," *High Technology*, January 1984, pp. 43-50; and Donald B. Keck, "Single-mode Fibers Outperform Multimode Cables," *IEEE Spectrum*, March 1983, pp. 30-37.

[25] "For good descriptions of the technology involved see: Duane L. Huff, "Cellular Radio," *Technology Review*, November/December 1983, pp. 53-62; George R. Cooper and Ray W. Nettleton, "Cellular Mobile Technology: The Great Multiplier," *IEEE Spectrum*, June 1983, pp. 30-37; and Television Digest, Inc., *Cellular Radio–Birth of an Industry, 1983.*

phone company and a radio communications company, in each area. Subsequently, the FCC received almost 400 applications to provide service in the 30 next largest markets and 567 applications to provide service for the next 30 markets.[2e]

Market analysts expect that the demand for cellular service will be large-driven by people who want to communicate while on the move. Cellular phones provide quality communications, and the current high cost will decrease. Some predict that the cost will drop to $500 per phone within 5 years.[27] Service charges started out around $150 per month, but are dropping fast.[28] The technology on which cellular phones are based is capable of providing additional services, e.g., data terminals and printers in a briefcase; public cellular phones on trains, buses, and planes; answering and message services; dictation services; and automatic callback.[29] In addition, encryption devices to protect privacy are now available.

Development of the radiotelephone system has been under way and may be available soon, subject to FCC approval. This system does not need an elaborate transmitter system and would be cheaper than a cellular phone. Radiotelephones can work either as a telephone or as a car-to-car radio. Although radiotelephones have a limited range, users can subscribe to a repeater service that picks up weak signals and rebroadcasts them. Radiotelephones (as well as cellular radios) are subject to eavesdropping. In addition, police scanners that can listen in on personal radiotelephone conversations are now on the market.[30]

Cordless Phones.—The cordless telephone is designed to meet a perceived consumer interest in being able to talk on the phone while walking around the house or in the yard. With the cordless phone, oral messages are no longer transmitted from the receiver to the network via a line, but instead are transmitted between receiver and base station via radio. These transmissions can be picked up accidentally on a home or car radio, and also can be intercepted easily by someone who wants to eavesdrop.

Companies marketing cordless phones and the FCC are well aware of the difficulty in ensuring the privacy of cordless phone calls. The FCC now requires that such phones be labeled with a warning that the conversation may be accidentally overheard. One reason cited for the lack of market interest in cordless phones is that customers desire privacy for their phone calls.

Private Carriers.–Until deregulation of the telephone industry, the market was dominated by common carriers that offered telecommunications services to any potential customer. Because of regulatory restrictions, capital investment requirements, and economies of scale, it was very difficult for an individual or company to set up a phone system. However, deregulation coupled with technological advances now make it possible to set up private telecommunications systems, which serve a specific business or a predetermined group of customers. Parties can also lease dedicated lines from the telephone company or private providers, form local area networks (LANS), and purchase private branch exchanges (PBXs). This variety of phone systems is not reflected in current laws that speak primarily to common carrier systems.

2. The contents of phone conversations that are transmitted in digital form or that are conducted on cellular phones or cordless phones are not clearly protected by existing statutory and constitutional prohibitions on the interception of phone calls.

The major statute prohibiting unauthorized interception of phone calls, Title III of the Omnibus Crime Control and Safe Streets Act, was written at a time when phone calls were transmitted in analog form, over wires maintained by common carriers. The technological changes discussed above have raised a series of questions about the scope of Title III and the possible need for new legislation. The present le-

[26] Huff, op. cit., pp. 59-60.
[27] Television Digest, Inc., op. cit., p. B-8.
[28] Huff, op. cit., p. 60.
[29] Huff, op. cit., p. 61.
[30] Benn Kobb and Lee Greathouse, "Car Radiotelephones Get Personal," *High Technology*, November 1984, pp. 18-21.

gal status of these new technologies is outlined below.

Digital/Data Communications. -Title III covers only the "aural acquisition" of an oral or wire communication, not the acquisition of communication in digitized form or data communications. Recent court rulings have not expanded the scope of Title III to cover digital or data communications. In *United States v. New York Telephone Co.,* 434 U.S. 159 (1977), the Supreme Court held that to be covered by Title III, a communication must be capable of being overheard. In 1978, the Fourth Circuit in *United States v. Seidlitz, 589* F.2d 152, ruled that nonaural communications were not protected by Title III.

Although it is clear that Title III does not cover data communication,[31] there has been some discussion whether Title III would cover phone conversations that are being transmitted in digital form.[32] Most interested parties, e.g., AT&T and the ACLU, now appear satisfied that conversations that are transmitted in digital form are covered by Title III because the interception is still aural and therefore covered by the statute. The Justice Department's position is similar, i.e., the analog-digital distinction is not important and that Title III applies to all phone conversations carried over the wires. Title III focuses not on the method by which communication is transmitted, but on the type of acquisition of that information. Since the Government's interception is aural, it does not matter for Title III purposes whether the transmission was analog or digital or by some other means. However, the courts have not ruled on the coverage of phone conversations carried in digital form and clarification by statute would avoid future legal misinterpretations.

The Foreign Intelligence Surveillance Act of 1978 (FISA) does require a court order for interception of digital conversations. Phone conversations being transmitted in digital form would be protected against unauthorized surveillance if the interception was for intelligence purposes. FISA does not cover law enforcement surveillance.

Section 605 of the Communications Act of 1934 does not provide any protection against unauthorized acquisition of digital wire communications because the courts have ruled that Congress intended Title III to be the exclusive remedy with respect to telephone inperceptions.[33]

Attempts to afford legal protection against the interception of digital or data communications through statutes that prohibit theft are likely to be futile because it is difficult to calculate or prove the informational value taken from the person whose communication is intercepted.

If no statute covers the interception of digital phone conversations, there may still be constitutional protection in the fourth amendment's "expectation of privacy" against unreasonable searches and seizures.

Cellular Telephones.–The issue of whether the interception of cellular phone calls comes under any existing statute, and thus requires some form of court order, has not yet come to the courts. In *United States v. Hall, 488* F.2d 193 (9th Cir. 1973), the Ninth Circuit Court held that Title III protects any communication that is transmitted in part by wire. The Court ruled that a telephone call from a mobile telephone to a landline telephone is protected by the statute, but that a phone call from a mobile telephone to another mobile tele phone is not. The Court characterized this as "an absurd result, " but one required by the statute. Based on the reasoning of the courts in other cases involving radio transmissions (cordless telephones and beepers), Title III and FISA would not apply because the communication was not a wire transmission, and Section 605 would not apply both because of Title III preemption and because cellular telephones use radio, not wire, transmissions. The posi-

[31] In ch. 4, *Electronic Mail Surveillance,* more detailed attention will be given to data communication.

[32] David Burnham, "Loophole in Law Raises Concern About Privacy in Computer Age, " *New York Times,* Dec. 19, 1984, p. A-1.

[33] See: *Watkins v. L. M. Barry& Co., 704* F.2d 577 (5th Cir. 1983) and *United States v. Hall,* 488 F.2d 193 (9th Cir. 1973).

tion of the Justice Department is to secure a Title III warrant before interception because one cannot tell whether the receiver is on a landline phone and hence using telephone wires.

Cordless Telephones.–The status of the protection afforded communication over cordless phones from unauthorized interception is not clear. Two State courts have ruled on the question. In 1984, the Supreme Court of Kansas, in *Kansas v. Howard, 679* P.2d 197, held that the user of a cordless telephone had no fourth amendment "expectation of privacy" and that interception of such communication does not violate Title III. The Court did not address the question of the expectation of privacy of the other party to the conversation. The Rhode Island Supreme Court has recently handed down a similar ruling in *Rhode Island v. Delaurier, 488* A.2d 688 (R.I. 1985). The Justice Department position is that investigatory authorities should get a Title III warrant before intercepting conversations carried over a cordless telephone. It may be important to note that in many instances the information resulted not from the Government actively listening to cordless phone calls, but from neighbors who picked it up on an FM radio dial and turned the information over to Government authorities.

Private Carriers.–Communications carried over private carrier communications systems are not "wire" communications under Title III. In addition, the AT&T consent decree may remove the regional holding companies from the category of common carrier engaged in interstate commerce as defined by Title III, and thus remove these companies from Title III coverage." Given the market trend toward private carrier systems and combination common-private systems, the implications of the current legislative distinction need to be explored for Title III, Sections 605 and 705(a) of the Communications Act, and FCC regulations.

[14]Bruce E. Fein, "Regulating the Interception and Disclosure of Wire, Radio and Oral Communication: A Case Study of Federal Statutory Antiquation, 22 *Harvard Journal on Legislation* **47, 69** (1985).

3. Interception of the content of phone calls represents a substantial threat to civil liberties, but also a significant potential benefit to investigative authorities. This is reflected in the standards and procedures presently embodied in Title III for such interception.

The following discussion uses the framework developed in chapter 2 (see table 6). In terms of the nature of the information acquired, the content of intercepted digitized phone communications is quite specific, detailed, complete, and often of a personal nature. The nature of the information that can be acquired does not vary with the system of transmission, the phone used, or the phone network.

The "private" v. "public" nature of the phone call does not differ at all based on the system of transmission or the phone network employed. It does differ somewhat according to the phone used, in that cellular and cordless phones using radio transmissions are inherently more vulnerable to interception, and thus more public. However, because a communication may be more readily overheard does not necessarily mean that investigative authorities should be able to intercept it with less authorization than for other calls.

The scope of surveillance is the same regardless of the system of transmission, phone used, or phone network employed. In any case, all parties to a phone call are generally overheard.

It is virtually impossible for an individual to detect whether or not the content of a phone call is being intercepted when the interception involves passive reception over the air signals. Again, this is true regardless of the system of transmission, phone used, or phone network employed.

The pre-electronic analogy will most likely be to analog transmission of phone calls made on conventional phones via a common carrier. Such calls are accorded a high level of protection against interception as reflected in Title III.

The governmental investigative interest in intercepting the content of phone calls is quite high. Knowledge of the content of phone calls

would be useful for any type of investigation, at any level of suspicion, and with or without more traditional techniques. As there is a history of policy in this area, extension of protection could arguably be consistent with what now exists.

4. OTA has identified three major options for congressional consideration with respect to policy on interception of the content of telephone calls: a) treat all phone calls similarly from the perspective of the extent of protection against unauthorized interception, i.e., extend Title 111 to cover all phone calls whether analog, digital, cellular, or cordless; b) formulate specific policies depending on the technological constraints and possibilities; and c) do nothing and leave the development of case law to determine policy, depending on individual circumstances.

Each of these options is discussed below in terms of the dimensions developed in chapter 2 (see table 6).

Option A.–The basic rationale for treating all phone calls similarly is that a phone call is a phone call. Therefore, regardless of the system of transmission (digital or analog, wire, satellite, microwave, or fiber optics), the phone used (conventional, cordless, or cellular), and the phone system employed (common carrier or private), phone conversations would be accorded the same protection.

There are two advantages to this approach. The first is that both individuals and investigative authorities would know their rights and responsibilities. A clear policy would disadvantage no one. The second is that the policy incorporates a standard that endures beyond technological changes. If a new type of phone is invented, or a new system for transmission of phone calls, the legal status would be clear to manufacturing companies, customers, investigative authorities, and the courts. Future confusion would be avoided.

Another strong argument for treating all phone calls similarly is that they have been accorded a historical expectation of privacy. Administrative and legislative actions prior to passage of Title III, experience with Title III, and public opinion over time are all supportive of protection for the privacy of phone calls. The analogy here is quite direct.

With respect to the governmental investigative interest involved and the stage of investigation at which it would be appropriate to allow interception, the standards developed in Title III for law enforcement and in FISA for intelligence purposes could be used for all phone calls. The standards for interception of phone calls for purposes of the proper administration of Government programs have not been formulated and are in need of legislative attention.

Option B.–The advantage of formulating specific policy depending on the technology involved is that policy would directly address the peculiarities of each technological situation. Policy would be precise. However, this option has three disadvantages. First, there will necessarily be a period in which there is no policy and in which the temptation will be to wait and see how the technology develops and what marketing is successful. Second, Congress will repeatedly be asked to deal with similar issues on which it will have to build individual hearing records and a separate consensus. Third, if Congress does not act quickly enough, the courts will be called on to set policy.

If this option were chosen, the standards relevant to each technology appear to be as follows:

Digital/Data Communications. -Based on the nature of the technology, the policy principles that exist in case law and legislation, and the investigative practice to date, there appears to be no reason to treat phone communications transmitted in digital form differently from those transmitted in analog form. The preponderance of evidence indicates that data communications are also in need of statutory protection against unauthorized interception. The Senate Judiciary Committee's Subcommittee on Patents, Copyrights and Trademarks held hearings on this issue on September 12, 1984. Witnesses from the Justice Department,

AT&T, and the Cellular Communications Industry Association stated the need to develop legislation protecting data communications.

The easiest and most direct policy alternative may be to amend Title III to include data communication. In October 1984, Representative Robert Kastenmeier introduced the Electronic Surveillance Act of 1984, which extended Title III definition of "intercept to include the nonaural acquisition of the contents of such communications. The Kastenmeier bill was reintroduced in the U.S. House of Representatives in September 1985 as the Electronic Communications Privacy Act of 1985 (H.R. 3378). A similar bill (S. 1667) was introduced in the U.S. Senate by Senator Patrick Leahy.

Additionally, it should be noted that computer crime legislation may also affect the security of data and data communications against unauthorized interception.

Cellular and Cordless Phones.– In designing policy for cellular and cordless phones, three separate issues need to be addressed. First, should the content of cellular and cordless phone calls be accorded a lower level of protection because the technology makes it easier to overhear such calls? If the answer is yes, then a standard based on the governmental investigative interest in intercepting such communications and the stage of the investigation needs to be fashioned.

The second issue is whether the caller and receiver should be accorded the same protection. The party using the cellular or cordless phone may know that the conversation can more easily be overheard. The other party most probably assumes that the conversation is via a conventional phone and that the usual protections apply, although under the concepts of one-party consent and assumption of risk, it is possible that the other party may not have a fourth amendment expectation of privacy. The Supreme Court's ruling in *United States v. White, 401* U.S. *745 (197),* that such practices as governmental encouragement and exploitation of misplaced personal confidence does not implicate the fourth amendment's guarantees would also appear to support this. In the Kansas cordless telephone case, the Court held that the user of a cordless phone has no expectation of privacy, but did not discuss the expectation of the other party. Under traditional principles of equity, it is necessary that the expectation of privacy for both parties be established and known in advance.

A third issue relates to the tracking potential of cellular phones. By monitoring the switching of cellular phone calls from one frequency to another, the cellular carrier can determine the location of individuals placing and receiving calls. Moreover, some companies record this information in a computer for billing purposes. At this time, precise locations cannot be determined because the cell sizes are large, but as cellular phones become more popular, cell sizes will be reduced allowing more precise tracking.[35]

The issue of tracking individuals by monitoring cellular phone calls could be dealt with by requiring investigative authorities to get a court order before getting such records from the cellular company. The standards for governmental investigative interest and stage of investigation at which this is considered appropriate would need to be addressed in legislation. Additionally, the legislation could require the cellular carrier to inform potential customers of its policies with respect to customer privacy. The model for such legislation could be the Cable Communications Policy Act.

Private Carriers.-The trend toward private carriers and combined common and private carrier systems throughout the telecommunications field indicates that the legal distinction between common and private carriers may no longer be valid. It appears that the distinction is based on a market configuration that is now outdated. Congress could enact legislation that applies equally to common, private, and hybrid communication systems.

[35] Robert L. Corn, "The Privacy Issue. " *Telocator,* September 1984.

Option C.—To do nothing and leave case law development to determine policy, depending on individual cases, has two serious disadvantages. The first is that, given the universal use of the phone system as a means of communication, lack of clear policy could lead to continued uncertainty and confusion as to the privacy accorded phone calls. The second is that major telecommunications changes are now occurring, and a belated response from Congress could detract from industry stability and growth.

5. New information technologies have also greatly increased the ability to collect and access transactional information about telephone calls, for example, the numbers and places dialed.

Because of the technological sophistication of the phone system, information on the numbers dialed and length of phone calls exists in real time and is stored for billing and administrative purposes. Access to this information makes it possible to determine patterns and interconnections in phone transactions.

Pen Registers.-Pen registers are devices that are attached to a telephone line to record the dialed pulses based on equipment that senses changes in magnetic energy. With a rotary phone call, a very sensitive radio receiver some distance from the wire can also pick up the pulses. Deciphering the numbers dialed by touch-tone phones is somewhat more difficult because the magnetic energy is weaker. Induction coils attached directly to the wire can pick up the signals, but radio receivers cannot.

Pen registers can pick up the number dialed and the length of the phone call. With a reverse phone book, one can then determine the party that was called. In order to install a pen register, one needs the cooperation of the phone company. Each pen register costs about $4,000 to install and monitor, depending on the length of time it is installed.

Automatic Billing Equipment.–With computer-controlled electronic switching systems, it is not necessary to use a pen register to determine calls dialed. Instead, the switch controller can automatically collect information on all calls, toll and flat rate. This can be done for both online data (real time) and for billing purposes. The information is retained on tape and can be accessed when needed.

6. Transactional information about phone calls (e.g., numbers and places dialed) is not clearly protected under existing statutes and judicial precedents on surveillance. Yet access to such information represents a significant threat to civil liberties and a significant potential benefit to investigators.

Title III was directed at the interception of the substance of phone calls and did not address the question of interception of numbers dialed. Transactional information is becoming more valuable as more of it is available and can be cross-referenced.

Pen Registers.–Given the present Supreme Court interpretation of Title III, Government officials do not need a Title III warrant to install pen registers. In 1977, the Court ruled in a 5-4 decision in *United States v. New York Telephone Co.,* 434 U.S. 159, that the FBI did not need a Title 111 warrant to use pen registers because the pen register intercepted nonaural communications and because the legislative history of Title III indicated that Congress intended to exclude pen registers.

Given the present Supreme Court interpretation of the scope of the fourth amendment, an individual cannot claim an expectation of privacy that numbers dialed will remain free from Government interception. The Court reached this ruling in *Smith v. Maryland,* 442 U.S. 735 (1979), in which it argued that Smith assumed the risk that the phone company might reveal all the numbers he dialed.

According to the Justice Department, the Foreign Intelligence Surveillance Act requires that law enforcement officers obtain a court order before using a pen register.[3G] The Justice Department currently requires its investigative departments to obtain a court order before installing a pen register. However, the

[36]John Keeney of the U.S. Department of Justice, Statement Before the Subcommittee on Patents, Copyrights and Trademarks of the Senate Judiciary Committee, Sept. 12, 1984.

court order does not require evidence of a link to illegal activities and does not require judicial review of the reasons for the pen register. Its purpose is to secure the cooperation of the telephone company. The court order generally authorizes the pen register for 30 days. Other Federal agencies appear to follow the Justice Department's guidance on this matter.

Automatic Billing Information.—The information that the telephone company retains for billing purposes and the information that is sent to customers on their bills is currently available to investigative authorities if the company chooses to cooperate in relinquishing the information. The telephone company's position has been that it will not release information without a court order or subpoena. Based on the Court's ruling in United *States v.. Miller,* 425 U.S. 435 (1976), it is difficult to see how an individual could successfully argue that he or she had a privacy interest or property right in this information.

Investigative authorities can generally get billing information from the phone company with a court order or a grand jury subpoena, which does not require probable cause. Recently, the Federal Government announced a plan to monitor long-distance telephone transactions from Federal offices with computer software that can be programmed to select specific information, e.g., phone calls to Dial-a-Joke, Sports Highlights, and Reno, and phone calls over a certain duration or at certain times of the day. The President's Council on Integrity and Efficiency is carrying out this program to reduce the Federal phone bill by discouraging and detecting abuse. " Some have criticized this program because of the possibility that phone calls to congressional offices and news reporters may be monitored as well.

Civil Liberties v. Governmental Interests. In terms of the dimensions introduced in chapter 2 to determine the threat to civil liberties from a particular surveillance technique, the nature of phone transactional information is less personal than the content of phone calls and may, therefore, deserve a lower level of protection. The nature of the information will vary depending on whether it is real-time information, in which case the present location of both parties is also divulged, or historical information. The former would appear to warrant more protection as it is more specific.

With respect to the public or private nature of the communication, transactional information is never considered public information, but rather is proprietary information. Clearly, the phone company needs to keep this information for billing purposes, but this does not put the information in the public realm. The protection accorded transactional information may be less than information that is kept in the home, but it is arguably deserving of a high level of protection.

The scope of surveillance that results from monitoring phone transactions is quite broad in that all phone conversations made are picked up by a pen register or recorded by the phone company. It would be difficult to minimize the scope of the monitoring, unless investigative authorities knew ahead of time the numbers they were interested in or the most likely times that relevant calls would be made,

It is very difficult at present for individuals to detect that their phone transactions are being monitored by investigative authorities. In fact, in order to learn of such monitoring, they would be dependent on the phone company or the Government. It would be fairly easy to give individuals notice of the circumstances under which phone transactional information would be sought and the uses that might be made of it.

In terms of pre-electronic analogies, such transactional information was generally not kept, not kept in detail, and/or not kept in a form that could be easily retrieved. It was, therefore, considered by individuals to be free from monitoring, The closest historical analogy to the monitoring of transactional information for surveillance purposes may be the use of mail covers.

[1] See William Safire, "Thanks for Calling," *New York Times,* Mar. 7, 1985; and Elizabeth Tucker, "U.S. to Eye All Federal Phone Calls," *Washington Post,* Mar. 9, 1985.

Information on phone transactions is potentially of great interest to investigative authorities. The Justice Department and other investigative agencies use such information primarily in the initial investigation of a case to determine whether activities of an implicating nature are occurring. Real-time information on phone transactions is also valuable in determining the location of parties, and is, therefore, valuable at any stage of an investigation. There are no traditional techniques for obtaining this information. A related OTA study on "New Communications Technology: Implications for Privacy and Security" is exploring telephone monitoring issues and policy options in greater depth.