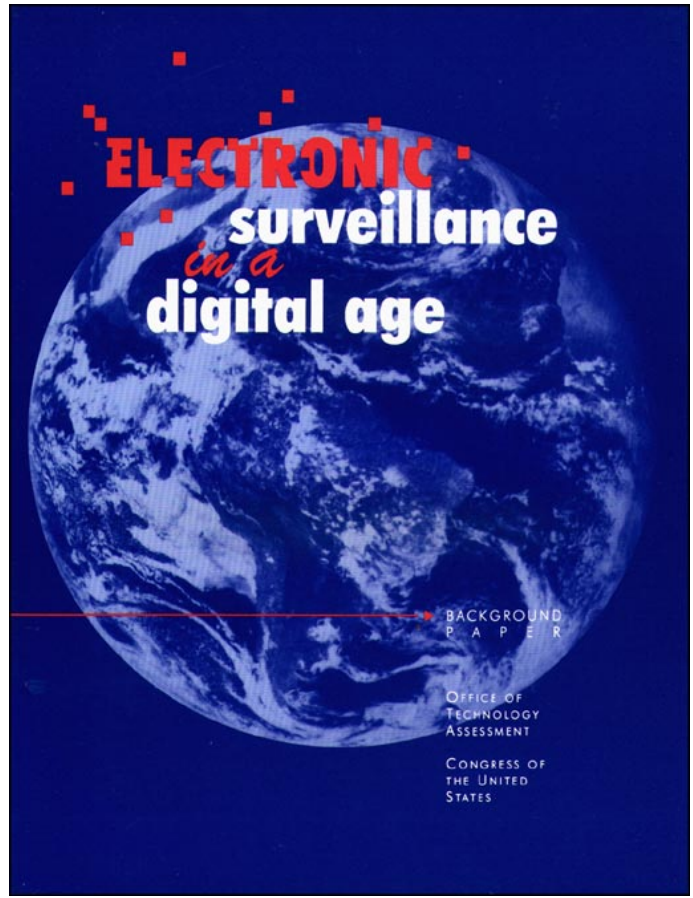
Electronic Surveillance in a Digital Age

July 1995

OTA-BP-ITC-149
GPO stock #052-003-01418-1



Recommended Citation: U.S. Congress, Office of Technology Assessment, *Electronic Surveillance in a Digital Age*, OTA-BP-ITC-149 (Washington, DC: U.S. Government Printing Office, July 1995).

Foreword

Lawlessness and terrorism present new challenges to our society as the 21st Century approaches. Electronic surveillance is an invaluable tool in America's arsenal to fight crime in this era of high-speed, global communications.

Digital communications technology has recently outpaced the ability of the law enforcement agencies to implement court authorized wiretaps easily and effectively. To address this problem, the 103d Congress enacted the Communications Assistance for Law Enforcement Act (P.L. 103-414). This Act invokes the assistance of the telecommunications industry to provide technological solutions for accessing call information and call content for law enforcement agencies when legally authorized to do so.

The law enforcement community and the telecommunications industry are currently working collaboratively on solutions to implement the requirement of the Act.

On September 27, 1994, Congressman Michael G. Oxley, a member or OTA's Technology Assessment Board, requested that OTA consider the technical aspects of implementing the law that will affect the ultimate cost to the government, the industry, and the rate payers.

This background paper reviews the progress of the industry and the law enforcement agencies in implementing the Act since its approval in October 1994. OTA extends its thanks to the Alliance for Telecommunications Industry Solutions (ATIS) that sponsors the Electronic Communications Service Providers (ECSP) committee, which is the forum for the collaborative efforts of the industry and law enforcement in seeking solutions for complying with the requirements of the Act. Without the willful cooperation of the ECSP, OTA would likely not have been able to accurately compile the information contained in this background paper.

Special acknowledgment is also given to the law enforcement community for its assistance that was extended through the Telecommunications Industry Liaison Unit (TILU) of the Federal Bureau of Investigation.

ROGER C. HERDMAN
Director

Project Staff

Peter D. Blair
Assistant Director, OTA
Industry, Commerce, and
International Security Division

Andrew W. Wyckoff
Program Director
Industry, Telecommunications,
and Commerce Program

JAMES W. CURLIN
Project Director

ADMINISTRATIVE STAFF

Liz Emanuel
Office Administrator

Karry Fornshill
Secretary

Diane Jackson
Administrative Secretary

Karolyn St. Clair
PC Specialist

PUBLISHING STAFF

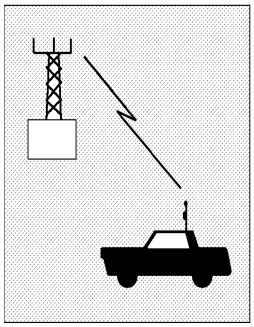
Mary Lou Higgs
Manager, Publishing Services

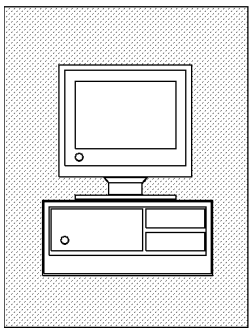
Chip Moore
Production Editor

Dorinda Edmondson
Electronic Publishing Specialist

Susan Hoffmeyer
Graphic Designer

Contents



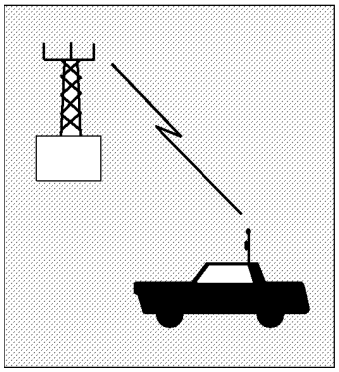


Summary and Discussion 1

The law enforcement community considers electronic surveillance[1] to be an invaluable tool for fighting crime. Officials cite many instances where criminal activities were either subverted, or if crimes were perpetrated, those responsible were apprehended as a result of court-approved electronic surveillance by law enforcement agencies.

The use of court-authorized electronic surveillance became increasingly more important as the telephone system became a part of everyday life. For many years the law enforcement community successfully matched its ability to perform electronic surveillance with the development of telephone technologies. The telephone industry worked cooperatively with law enforcement agencies to ensure that access to specific communications was available when the courts authorized such access.

When the telephone system was largely a network that connected handsets like the plain old black rotary dial telephones, wiretapping was largely a simple procedure of physically connecting a listening or monitoring device to a circuit associated with a telephone number. It was simple and inexpensive. But times have changed. Technology has raced ahead, the structure of the industry has changed, the number of carriers and services has multiplied; dependence on communications for business and personal life has increased, computers and data are becoming more



[1] For the purpose of this report electronic surveillance is considered to consist of both the interception of communications content (wiretapping) and the acquisition of call identifying information (dialed number information) through the use of pen register devices and through traps and traces.

important than voice traffic for business, and the nation has become enthralled with mobile communication.

In 1984, AT&T was divested of its regional operating companies that made up the Bell System in an antitrust settlement. Before then the American telephone system operated on standards and procedures set by AT&T, with equipment that was either built by its manufacturing affiliate or approved for use by the company. The system worked uniformly and predictably throughout the United States.

Prior to divestiture, the telephone system was largely based on analog technology, with calls originated and terminated over copper wires or cables, which were directed to the receiver by electrical contact switches. Microwave, and later satellite, communications spanned distances that copper did not cover through the 1960s. Those days are gone. Analog technology is being replaced by digital technology, optical fiber is rapidly replacing copper cable, and computers are replacing electrical switches for directing and processing calls.

Computers are increasingly used to communicate with other computers that transmit and receive digital data and messages. Facsimile, still an analog-based technology, has grown remarkably as a preferred means of communication. Wireless technologies, like cellular telephones, have loosed the caller from the restraints of the telephone line, and has allowed freedom to communicate from autos, trains, boats, airplanes, and on foot. In the future it is expected that personal communications systems will allow anyone, anywhere, to place phone calls via satellite linked to the ground communication system. These developments have been precipitated by letting the innovative zeal of private entrepreneurs seek their own visions of what the technology should be after the divestiture or AT&T and the deregulation of the telephone industry. Many of the new developments have been made possible through the application of digital technology.

Transition from an AT&T-regulated monopoly to the telecommunications system of the future—i.e., a digitally based National Information Infrastructure (NII)—has been a process of chaotic development. No longer do proprietary standards and operating protocols of a monopoly provider determine the architecture, functions, and procedures of the national telecommunications system. Neither is it a certainty that one telecommunication device, standard, or transmission protocol will work with another. Nor is there uniform delivery of compatible and interoperable services, e.g., Integrated Systems Digital Network (ISDN), to all quarters of the country. Each of the Regional Bell Operating Companies (RBOCs), the independent telephone companies, the interexchange (long-distance) carriers, and the private competitive-access providers each have their own business plans and schedules for deploying technologies. The United States has traded the comfort of uniformity and predictability in its communication system for creative innovation and vigorous competition. The technological payoff for divestiture and deregulation has been large, but progress has not been without a price to the law enforcement community.

Access to electronic communications (both wire other electronic communications) for law enforcement, i.e., court-approved wiretaps, pen registers, and traps and traces, are not simple or routine procedures—neither technically, nor legally. (See box 1-A.)

Recent and continuing advances in electronic communications technology and services challenge, and at times erode, the ability of law enforcement agencies to fully implement lawful orders to intercept communications. These advances also challenge the ability of telecommunications carriers to meet their assistance responsibilities. Thus, law enforcement agencies are finding it increasingly difficult to deal with intercepted digital communication, which might now be voice, data, images, or video, or a mixture of all of them. Even the concept of the "telephone number," which at one time identified the target subject of the court-ordered wiretap and was tied to a physical location, may now only be a number that begins the communication, then loses its identity with an individual or location as the call may be routed to others by the caller. Subscribers

BOX 1-A: Procedures for Establishing a Lawful Wiretap

Legal Authority

The Fourth Amendment of the U.S. Constitution protects Americans against unreasonable search and seizure by the government. Each intrusion into the private lives of U.S. citizens by government entities must fit within the limits prescribed by the U.S. Constitution as interpreted by the U.S. Supreme Court.

The evolution of the telephone system and wiretapping is one of the best examples of where technological development continues to challenge the Court and the Congress in balancing personal rights with public needs, In 1928, the Supreme Court first confronted the issue of whether wiretaps constituted "search" or "seizure under the Constitution. *(Olmstead v. United States,* 48 S. Ct. 564, 277 U.S. 438) In the Instance of *Olmstead,* the Court found that tapping a telephone did not violate the Fourth Amendment The case IS best known, however, for the dissenting views of Justice Brandeis, who argued that wiretaps without a court order or warrant violated a person's right of privacy, which he defined as "the right to be let alone--the most comprehensive or rights and the right most valued by civilized men. " At the time of the *O/instead* decision there were no wiretap statutes.

The Congress attempted to deal with the issue in the Communications Act of 1934. Siding with Justice Brandeis' views, the Congress included in Section 605 of the Act the provision that "no person not being authorized by the sender shall intercept any communication and divulge or publish [its] existence, contents...or meaning. " A series of cases followed passage of the 1934 Act, which interpreted various technical aspects of the law dealing, e.g., the admissibility of evidence, interstate and intrastate distinctions affecting the law, and individual rights of the called and calling parties.

By 1968 the provisions of the Communication Act of 1934 dealing with wiretapping were so muddled by Interpretations of federal and state courts that the Congress decided to set forth a process and delimit the legal authority of the law enforcement community's authority to conduct wiretaps under Title Ill of the Omnibus Crime Control and Safe Streets Act of 1968. The procedures set forth in the 1968 Act define the authority and guide the conduct and procedures of wiretaps by federal law enforcement agencies. Thirty Seven states have enacted parallel state statutes that define wiretapping authority within their jurisdictions. Many of the states have laws more restrictive than those governing the federal authorities.

Telecommunications and computing technology continued to develop, so the Congress found it necessary to enact the Electronic Communications Privacy Act of 1986, which amended the Omnibus Crime Control and Safe Streets Act of 1968 by broadening its coverage to include electronic communications (to include electronic mail, data transmissions, faxes, and pagers). The provisions of Title Ill of the 1968 Act, as amended, continue to govern the procedures for obtaining legal authority for initiating and conducting a lawful interceptions of wire, oral, and electronic communications.

Procedure for Obtaining Court Order

It is more involved for law enforcement officials to obtain authorization to initiate and conduct a lawful wiretap than it is to obtain a search warrant. A normal search warrant requires only that a law enforcement official apply directly to a federal magistrate. Title Ill requires that a wiretap order be approved by the Attorney General, the Deputy, or an Assistant Attorney General of the Department of Justice before forwarding to a local U.S. Attorney for application to a federal district court or other court of jurisdiction. Electronic surveillance is only authorized for specific felonies that are specified in the Act, e.g., murder, espionage, treason, kidnapping, bribery, narcotics, racketeering, etc.

Applications for electronic surveillance must show probable cause set forth in specific terms. It must also be shown that the use of other normal investigative techniques can not provide the needed information, or that they would be too dangerous. The information in an electronic surveillance application must

(continued)

BOX 1-A (cont'd.): Procedures for Establishing a Lawful Wiretap

specifically state the offense being committed, the place or telecommunications facility from which the subject is to be Intercepted (special provisions are made for "roving" interceptions where the subject may be highly mobile), a description of the types of conversations to be intercepted, and the identities of the person or persons committing the offenses and who are the subjects of the intercept. Thus, the Act focuses on obtaining hard evidence to be used in prosecution, rather than general Intelligence

Court orders are normally valid for 30 days. Judges may also require periodic reports to the court advising it of the progress of the interception effort. A court may extend the order for an additional 30 days if justified. Federal district court judges can authorize electronic interceptions within the jurisdiction of the court where he or she presides. If the intercept subject is mobile or is using a mobile communications device a judge may authorize electronic surveillance throughout the United States wherever the subject may travel. A judge actually issues two orders. one authorizing the law enforcement agency to conduct the interception; the second directing the service provider to set up the Intercept, specifying the telephone numbers to be Intercepted and other assistance to be provided.

Under "emergency situations, " e.g., serious and life-threatening criminality as defined in the Act, the Attorney General and others specified in the Act, can authorize and emergency electronic surveillance that if valid Immediately, but application for a court order must be issued within 48 hours. If a court does not ratify the action and issue an order the intercept must be immediately terminated. Emergency intercepts are rarely initiated.

Preserving Privacy and the Integrity of the Evidence

Intercepted communications are required to be recorded in a way that wiII protect the recording from editing or alterations. Interceptions are required to be conducted in such a way as to "minimize the interception of communications not otherwise subject to interception. " This Included unrelated, Irrelevant, and non-criminal communications of the subjects and of others not named in the order.

Upon expiration of the intercept order, or as soon as practicable, the recordings are presented to the court of jurisdiction and are sealed. Within a reasonable time period after interception, the subjects must be furnished with an inventory of the recordings, and upon motion, a judge may direct that portions of the recordings be made available to the subject for inspection.

Should the law enforcement agency err in conducting the electronic surveillance as authorized in the court order, the intercept may be challenged, and if found to have been illegally conducted, the evidence in the intercept may be suppressed.

SOURCE Title III of the Omnibus Crime Control and Safe Streets Act of 1968

at fixed locations can program the central office to forward their incoming calls to other numbers during certain times of the day or days of the week or to forward or block calls originating from specific telephone numbers. Cellular telephones and the next generation of mobile communication, Personal Communication Services (PCS), enable the caller to travel over great distances while maintaining communications that are handed off to other service providers. Modem communication systems are no longer wires connected to a switch, but are digital lines linked to routing tables and computer databases that set up calls with other computers almost instantaneously. It is an era of intelligent networks, switch systems that do not require physical connections, a digital environment that allows sophisticated encryption, and a choice of communication modes from voice through video. Persons might not communicate verbally, but may instead use computers as intermediaries. Communication need no longer be immediate, such as a conversation among individ-

uals, but instead may be a computer message or a voice message addressed to a "mailbox" that may be stored, which can be accessed by another party at a future time.

Law enforcement surveillance has become more difficult and more expensive as a consequence of these new technological innovations. What was once a simple matter of initiating a court-approved wiretap by attaching wires to terminal posts now requires the expert assistance of the communication service provider. Even the once specific, but routine, requirements of the courts to authorize a wiretap are today more complex because of modern communication technology.

There has been a sea change in communication technology, and the law enforcement agencies find it difficult to maintain electronic surveillance as new services and features are added to the nation's communication networks. During the late 1980s and early 1990s, the Federal Bureau of Investigation (FBI) and other law enforcement agencies began to take steps to address the challenges posed by advanced telecommunications technologies and services. By 1992, it was evident that legislation would be necessary to ensure a level playing field and offer measures to address compliance, security, and cost recovery. During the 103d Congress, the Clinton Administration proposed legislation to clarify the technical assistance provisions of existing electronic surveillance statutes; and in October 1994, Congress passed and the President approved the Communications Assistance for Law Enforcement Act (P.L. 103-414).

The Act requires the telecommunication industry to assist the law enforcement agencies in matching intercept needs with the demands placed on them by modern communication technology. The Act does not change the authority of the courts to approve pen registers and traps and traces[2] as well as wiretaps, or for law enforcement agencies to execute them under court order.[3]

Recognizing that existing equipment, facilities, or services may have to be retrofitted to meet the assistance capability requirements, the law provides that the Attorney General may agree to pay telecommunications carriers for all reasonable costs directly associated with the modifications to those deployed systems. Accordingly, the Act authorizes the appropriation of $500 million over four fiscal years to reimburse telecommunications service providers for the direct costs of retrofitting those systems installed or deployed as of January 1, 1995. Generally speaking, costs for achieving compliance for equipment installed after January 1, 1995, are to be borne by the telecommunications carrier for compliance determined to be "reasonably achievable." The Act also allows for cost recovery for reasonable costs expended for making modifications to equipment, facilities, or services pursuant to the assistance requirements through adjustments by the Federal Communications Commission (FCC) to charges, practices, classifications, and regulations in response to a carrier's petition.

The combined cost to the telecommunication industry and to the law enforcement agencies is likely to be significant. However, supporters of the bill during the congressional debate over the Act in the 103d Congress cited the offsetting costs to society caused by crimes that might result in the absence of improving law enforcement's capabili-

---

[2] Pen register is an antiquated term. It stems from the manner in which the digits in a phone number were recorded when telephones used pulse dialing technology, which has since been replaced by touch-tone technology. The term still applies to the recovery and recording of the dialing information that addresses a call to and from an intercept subject. Authority for initiating a pen register or trap and trace surveillance is found in 18 USC 3123.

[3] Omnibus Crime Control and Safe Streets Act of 1968, Pub. Law No. 90-351, Title III. However, P.L. 90-351 only affects federal law enforcement agencies. Thirty-seven states have enacted some form of electronic surveillance laws to govern law enforcement agencies and courts within the state's jurisdiction. Many of the states' electronic surveillance statutes are more stringent than the 1968 Federal Act. The remainder of the states do not sanction wiretaps by their law enforcement entities.

ties to conduct electronic surveillance. Congress considered the balance of costs and benefits and determined that the benefits from crime prevention outweighed the costs of compliance.

Law enforcement believes that these costs will not have a significant impact on either the shareholders or the customers of the telecommunications industry. They contend that costs not compensated under the Act will be spread among customers, and that the impact on the average telephone bill will be insignificant. While this may or may not be true, the exact financial impact on the government, companies, and their customers will not be known until planning and implementation process as set forth in the Act. At the time of this report those costs are unknown.[4]

At a time when federal budgets are being trimmed, the cost of electronic surveillance is likely to increase sharply. Much of the cost of new technology installed after January 1, 1995, will be borne by the service providers and their subscribers. But there also will be a substantial financial burden placed on state, federal, and local law enforcement agencies to conduct and maintain surveillance after the new technology is in place. The Act does not address these costs.

CONGRESSIONAL REQUEST AND SCOPE OF THE STUDY

On September 27, 1994, Congressman Michael G. Oxley, a member of OTA's Technology Assessment Board, requested that OTA consider the cost factors of implementing the Communications Assistance for Law Enforcement Act (P.L. 103-414). In his letter requesting the study, Mr. Oxley observed that during the debate preceding enactment, the costs of the legislation and who should bear those costs were highly controversial issues.

Congress finally agreed to authorize $500 million over fiscal years 1995-98 for retrofitting the service provider's pre-1995 services, largely based on its already installed switches (the Attorney General may cover costs for new equipment based on technology that is not "reasonably achievable" as determined by the FCC). The $500 million was a compromise among widely ranging estimates from the telecommunication industry and the law enforcement agencies. Both the industry and law enforcement's estimates were based on assumptions about costs for modifying existing equipment and deploying the technology, but the estimates were generally not based on formal engineering cost analysis. OTA further found that, for practical purposes, it is not possible to develop reliable cost figures without knowing what specific capacities for electronic surveillance the law enforcement agencies will place on the service providers to meet their surveillance needs.[5]

The Act provides a process to obtain this information through the collaboration of the law enforcement agencies and the industry, but in the meantime, the clock is running on the compliance deadline, while the Attorney General's capabilities and capacity notification to the industry that will scope the requirements (and upon which costs to the carriers will be determined) is not due until October 1995. Priorities and capability statements that must be prepared by the industry in response

---

[4] On Aug. 11, 1994, Hazel E. Edwards, Director, Information Resources Management/General Government Issues, U.S. General Accounting Office, testified before the House Subcommittee on Technology and the Law, and the House Subcommittee on Civil and Constitutional Rights, stating, ". . .it is virtually impossible to precisely estimate the reimbursement costs discussed in this bill because costs will depend on evolving law enforcement requirements." After careful study of the technological and operational factors involved in meeting the requirements of the Act, and with information provided by the telecommunication industry and the law enforcement agencies in the course of compiling this study, OTA reaffirmed the findings and conclusions of GAO in this regard.

[5] The General Accounting Office (GAO) is assigned the responsibility under P.L. 103-414 (Sec. 112(b)(2)) provide cost estimates of the expenditures expected by the telecommunication carriers to comply with the requirements of the Act. The Comptroller General is to report to the Congress by Apr. 1, 1996, and every two years thereafter, progress for compliance with the Act and projections of future costs expected to be incurred.

to the Attorney General's notification will follow within 180 days. After this process is completed, it will be possible to estimate the immediate costs of complying with the Act.

This collaborative process involves two different types of organizations with differing goals. Law enforcement agencies would like to be able to execute authorized electronic surveillance without either technological impediments or delay. Telecommunications carriers, on the other hand, are reluctant to plan for modifications of their equipment and facilities without an expectation that they will be compensated for their costs. Consequently, in order to facilitate the collaborative process, both parties consider the appropriations authorized by the Act to be an important factor in its success.

This study considers the technical factors that will affect the rate of compliance with the requirements of the Act by the industry, and will provide insights into the technical components that will determine cost. OTA did not, and could not during the period of this study, develop an aggregate cost estimate for implementation of the Act. *Only after the Attorney General provides the notification of law enforcement's capacity needs to the service providers and equipment manufacturers, and engineering cost analyses are done, will reliable and meaningful cost estimates be available*. It is doubtful that such estimates will be available before the second quarter of 1996, given the time schedule under the act. However, the description of the technology and modifications required by the act as summarized in this background paper indicate the scope and complexity, and hence the likely subjective magnitude of the costs involved.

During the debate preceding enactment, considerable attention was given to sensitive issues of privacy and personal rights and protections. This report does not address these issues. OTA's commission to undertake this study considers only those technical factors that enter into the cost and deployment of the technologies required of the telecommunications industry by the Act and the operation of the National Information Infrastructure (NII) of the future as it may affect the surveillance missions of law enforcement agencies.

THE COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT (P.L. 103-414)

An affirmative obligation for telecommunication service providers to assist the law enforcement community in authorized electronic intercepts has existed since Congress amended Title III of the 1968 Omnibus Crime and Safe Streets Act in 1970.[6] This amendment clarified an ambiguity in the 1968 law about the specific responsibility of telecommunications carriers for assisting law enforcement agencies in authorized wiretaps.[7] The Supreme Court in *United States* v. *New York Telephone*, 434 U.S. 159, 177 (1977) found that 18 U.S.C. 2518(4) required the federal courts to compel telecommunication providers to provide "any assistance necessary to accomplish an electronic interception." The question of whether a carrier has any obligation to *design* its equipment to facilitate an authorized electronic surveillance under 18 U.S.C 2518(4) was never litigated.

It was not until the technology explosion in the communication industry in the 1980s made it more difficult for law enforcement agencies to conduct authorized wiretaps that the issue of design requirements arose. The Communications Assistance For Law Enforcement Act makes it clear that the service providers must now consider equipment and system *design* as well as the *capability* to provide the call content and call identification information needed by law enforcement

[6] *See* 18 U.S.C. 2518(4). The amendment requires the service provider "furnish. . .information, facilities, and technical assistance necessary to accomplish the interception. . . . ." The amendment further provides that a cooperating service provider ". . .be compensated. . .for reasonable expenses incurred in providing such facilities or assistance."

[7] In 1970 the Ninth Circuit Court of Appeals found the 1968 Act did not provide the necessary statutory authority of law enforcement agencies to compel the telephone companies to assist in wiretaps. (*Application of the United States*, 427 F. 2d 639 (9th Cir. 1970).

agencies, and the *capacity* that the law enforcement agencies need to simultaneously intercept a specified number of wiretaps. The Act also establishes a process for reimbursing the service providers for their expenses in meeting law enforcement's needs. (See appendix A, Section-by-Section Summary)

PRINCIPAL FEATURES OF THE ACT

Coverage and Exclusions

All "telecommunications carriers" that are considered common carriers must comply with the requirements of the Act.[8] This includes local exchange carriers, competitive access providers (CAPs), interexchange carriers, cellular carriers, providers of personal communication services (PCS), and other mobile radio services. Cable companies and electric utilities companies would be covered if they provide telecommunications services for hire to the public.

Companies providing "information services" are excluded from the Act's requirements. Such services include electronic messaging services, e.g., electronic mail, electronic forms transfer, electronic document interchange (EDI), information and databanks available for downloading by a subscriber, and Internet service providers.

Capabilities Required

A telecommunications carrier must have the capability to selectively isolate and intercept real-time electronic traffic and call identification information and deliver it in the appropriate format to law enforcement personnel off the carrier's premises. The service provider may not reveal the physical location of an intercept subject, other than that information available from a telephone directory number, unless so authorized by court order. A carrier must be able to notify a law enforcement agency, during or immediately after the transfer of control of the communication to another carrier. Carriers are not responsible for decryption unless they have provided that encryption service to the intercept target. (See figures 1-1A, 1-1B.)

Capacity Requirements

By October 25, 1995, the Attorney General must notify the carriers of the law enforcement agencies' specific capacity needs, i.e., the number of simultaneous interceptions that must be planned for within each service provider's system. This is expected to vary among the service providers, with higher capacities required in larger urban areas, such as the New York Metropolitan area, Miami, Los Angeles, etc., while few or no requirements may be placed on those carriers serving some rural areas. On the other hand, cellular and other mobile communication carriers may be required to equip a large proportion of their switches with wiretap capabilities so that taps on intercept parties may be linked as they roam among service areas.

The Attorney General must provide the carriers with two estimates of needed capacity:

a. an *actual capacity* that covers the period through October 25, 1998, and
b. an estimate of *maximum capacity* that would be required on October 25, 1998 and beyond.

The Attorney General is to periodically review law enforcement's needs and notify the industry of any changes in maximum capacity.

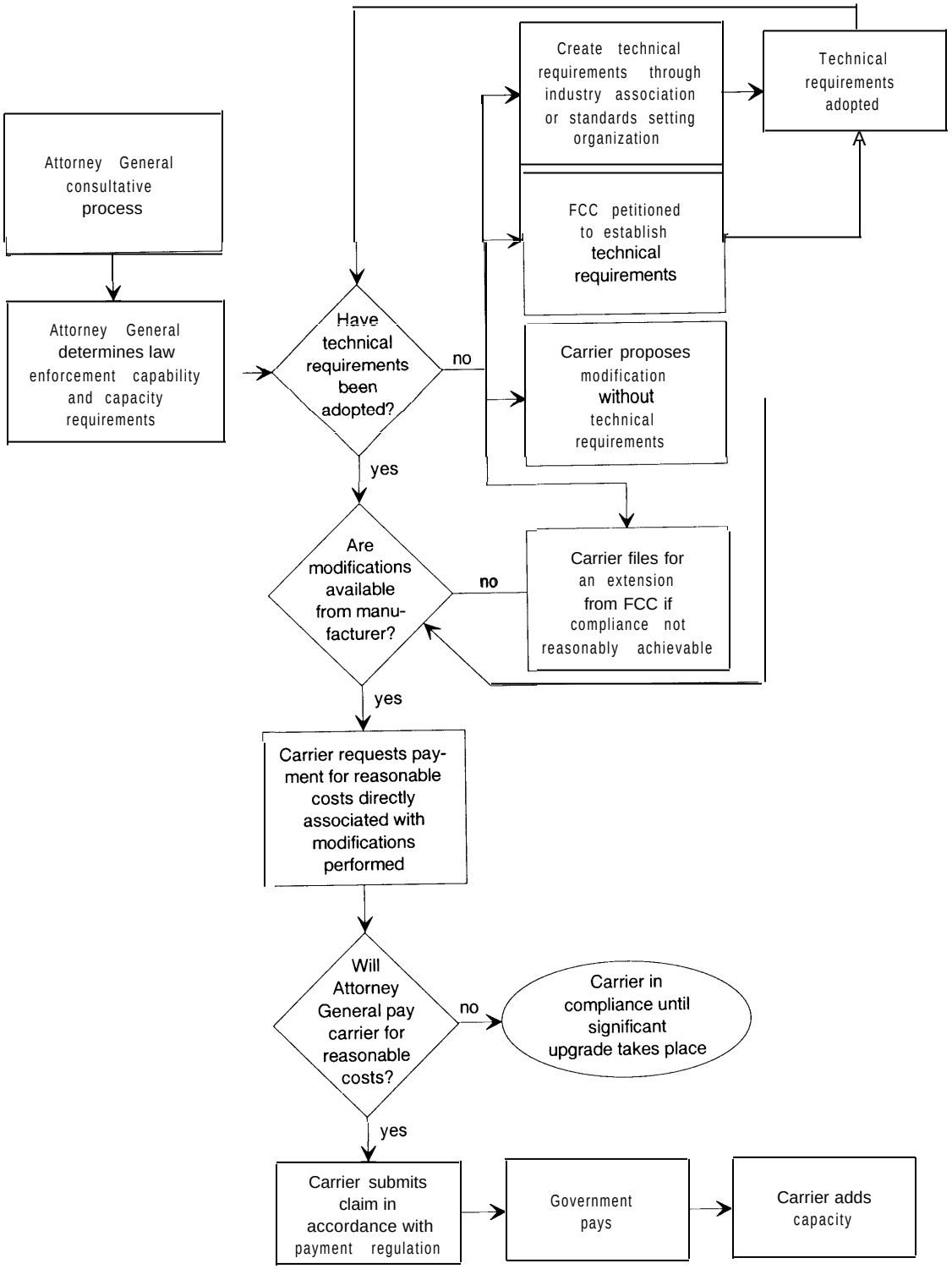
Within 180 days after the Attorney General publishes the capacity notifications, service providers must provide statements that identify those areas where the carrier does not have the capacity to simultaneously accommodate the types of surveillance required. (See figure 1-2.)

Time for Performance

Within three years after the Attorney General notifies the carrier of the initial capacity needed by the law enforcement agencies, a carrier must be able to provide the number of simultaneous intercep-

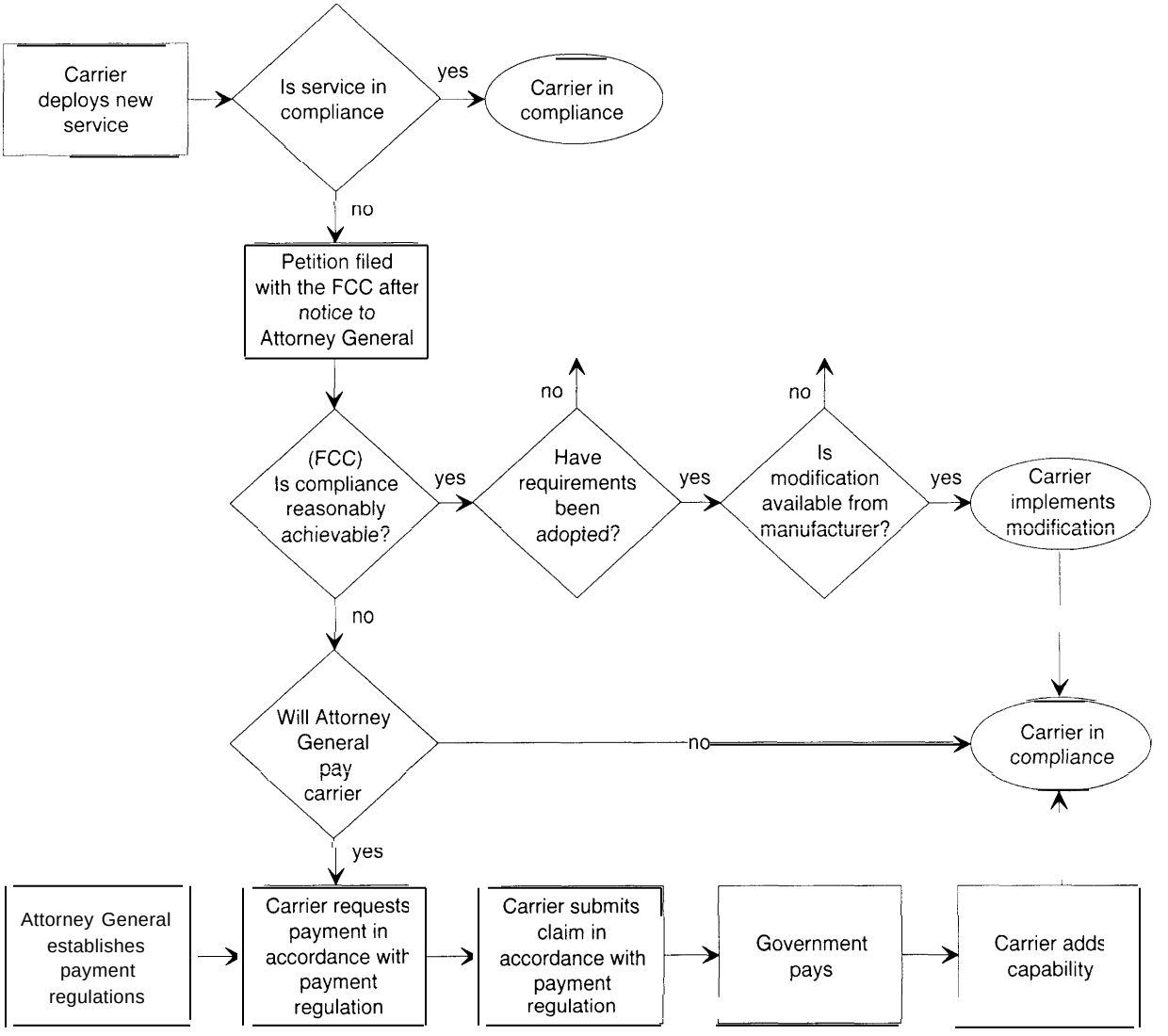
[8] A Common Carrier is a company that furnishes public telecommunications facilities and services, e.g., a telephone or telegraph company. A Common Carrier cannot control message content.

FIGURE 1-1A: CALEA Process to Meet LaW Enforcement Capability Needs On or Before January 1, 1995



SOURCE Federal Bureau of Investigation, 1995

FIGURE 1-1B: CALEA Process to Meet Law Enforcement Capability Needs After January 1, 1995



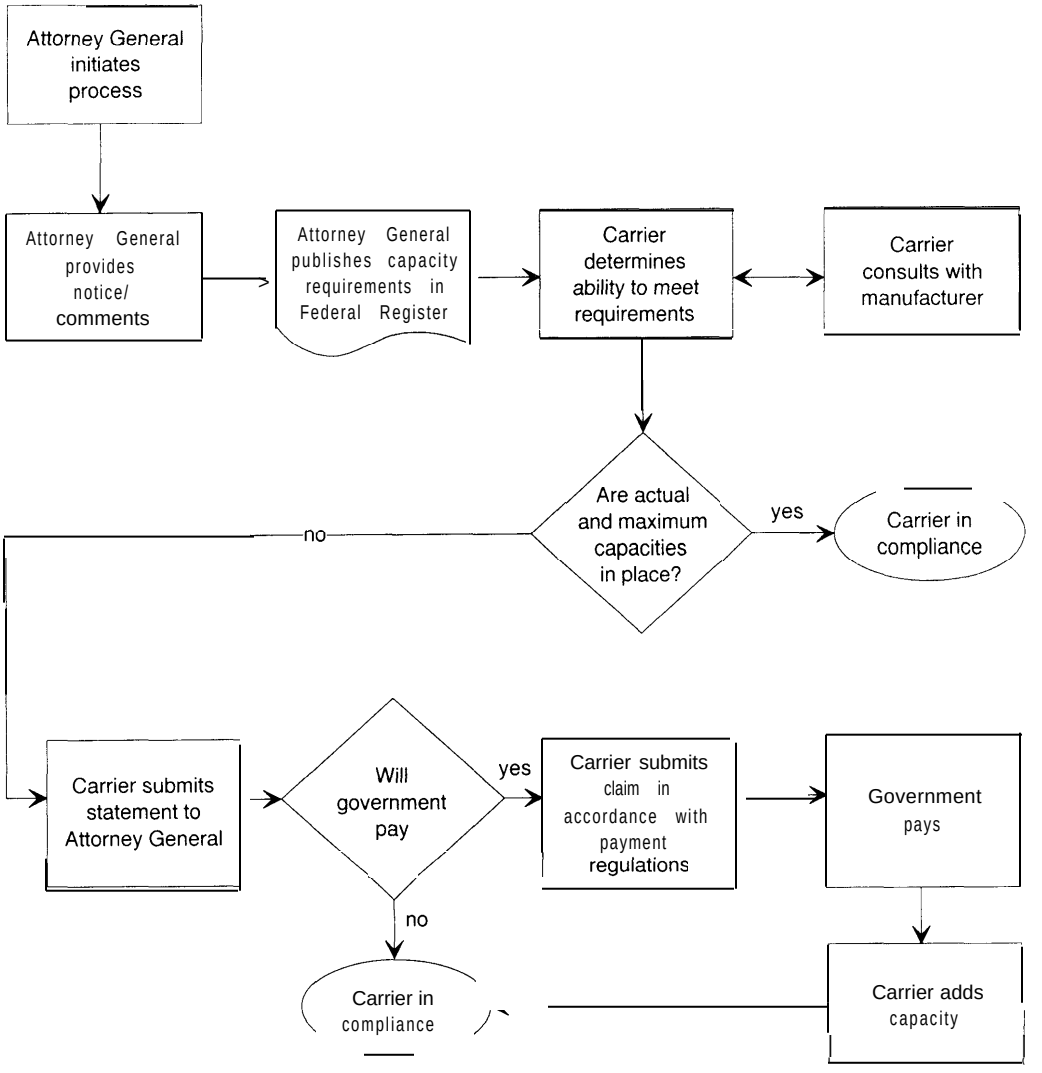
SOURCE Federal Bureau of Investigation, 1995

tions specified (this date will likely be in late 1998). After that time, service providers must be capable of increasing the number of simultaneous interceptions up to the maximum number determined by the Attorney General. A carrier may petition the Federal Communication Commission (FCC) for an extension of the compliance deadline if meeting the capability requirements is not *reasonably achievable* by the 1998 deadline. If the FCC agrees that compliance is not reasonably achievable within that time span, the FCC may grant an extension of up to two years (circa 2000). (See figure 1-3.)

■ Collaboration

Carriers, manufacturers, and vendors are encouraged to collaborate among themselves and with

FIGURE 1-2: Industry Process to Meed CALEA Capacity Needs

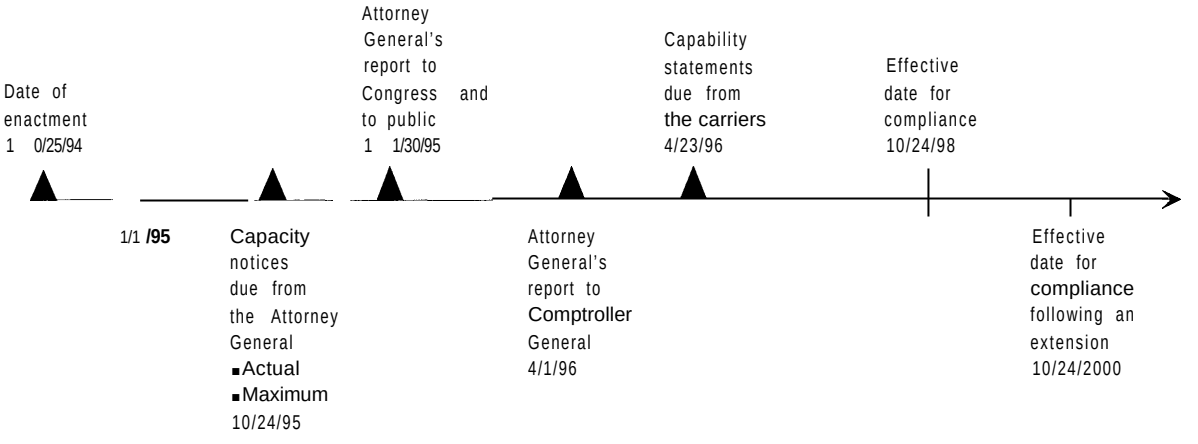


SOURCE Federal Bureau of Investigation, 1995

the law enforcement agencies in developing and modifying technology and equipment to meet law enforcement needs. The Attorney General represents the federal and state law enforcement agencies in the collaborative process. As the representative of law enforcement, the Attorney General must consult with industry associations, standards-setting organizations, telecommunication users, and state regulatory commissions to facilitate implementation of the Act. The Federal Bureau of Investigation (FBI) has been given the authority for implementing the Act.

Carriers and manufacturers are protected from the risk of being judged in noncompliance of the capability requirements if they adopt an accepted technical standard, or an agreed upon industry-government technical solution. However, the absence of such standards or technical solutions does not relieve the industry of its obligations under the Act.

FIGURE 1-3: Timeframe for the Implementation of the Legislation



SOURCE Federal Bureau of Investigation, 1995

If voluntary standards or technical solutions are not available, or if an adopted standard or solution is judged by anyone to be deficient, the FCC may be petitioned (by any person or entity) to establish the necessary technical requirements or standards to allow compliance with the Act.

■ Cost Reimbursement

The Attorney General is authorized to pay the direct costs for modification of equipment, facilities, or services necessary to meet the requirements of the Act for equipment deployed prior to January 1, 1995, and for costs of modifications after that date if they are determined to be not "reasonably achievable." Five hundred million dollars ($500 million) is authorized to be appropriated over four fiscal years, 1995 through 1998.[9]

If the Attorney General does not agree to reimburse a carrier that requests compensation, the carrier is considered to be in compliance with the Act until that equipment is replaced or significantly upgraded, or otherwise undergoes major modification.

For equipment deployed after January 1, 1995, a carrier must assume the expense of complying with the Act unless to do so is *not reasonably achievable,* i.e., that compliance would impose "significant difficult y or expense" on the carrier or users.[10] The FCC would determine whether compliance would be reasonably achievable or not.

If compliance is deemed by the FCC not to be reasonably achievable, the Attorney General may agree to pay the carrier for costs of developing the capability to comply with the Act. If the Attorney General does not agree to pay such costs, the carrier is considered to be in compliance with the Act.11

[9]The Congressional Budget Office (CBO) projected that outlays for the $500 million authorized by the Act would be $25 million for FY 1995,$100 million for FY 1996, and $375 million for FY 1997. Senate Committee on the Judiciary, Report on S.2375, The Digital Telephony Bill of 1994, Report 103-402, p. 33, 103d. Cong., 2d sess., Oct. 6, 1994.

10 If the Attorney General decides to pay the costs for modifications mad after Jan. 1, 1995, that are determined to be not reasonably achievable, the government is obligated to pay the carrier only "for the *additional* cost of making compliance with the assistance capability requirements reasonably achievable." [emphasis added]

11 Id., CBO estimates that additional authorizations of $100 million will be required for each of the fiscal years 1998, 1999.

The Act (through an amendment to the Communications Act of 1934) allows for cost recovery for continued compliance with the Act to be built into the rate structure for interstate and foreign communications under the jurisdiction of the FCC. (Sec. 229(e)) Tolls and rates for intrastate communications are largely determined by the states, and the Act does not directly address cost recovery through intrastate rate adjustment.[12]

Implementation of the Act

Since January 1992, when President Bush authorized the Department of Justice to proceed with legislation that led to the enactment of P.L. 103-414, law enforcement officials have been working with the telecommunication industry to solve the problems associated with electronic surveillance in a digital, high-speed communication environment.[13] In July 1992, the FBI, as spokesman for all federal, state, and local law enforcement agencies, published a document entitled *Law Enforcement Requirements for the Surveillance of Electronic Communication*. The document outlined law enforcement's requirements for the surveillance of electronic communications and still continues to guide the framework for government/industry collaboration, though updated several times since then.[14] (See appendix B.)

In general, the telecommunication industry has been compliant with regard to law enforcement's concerns for maintaining wiretap capabilities in the face of technological development. The major initial sticking point in complying with the need of the law enforcement community concerned who would be financially liable for meeting law enforcement's needs. The companies would not unilaterally invest money or technical resources to seek solutions to the problems in the absence of a legal mandate that would ensure that competing companies would be held to the same requirements. Many, but not all, of the industries' concern about reimbursement and fairness were dealt with in the legislation. Recently, however, the industry has been more concerned with how law enforcement's capacity requirements will impact costs, and hence their future financial liability.

The 1994 Act authorizes the appropriation of money for cost reimbursement to meet law enforcement's requirements, and contains a fail-safe provision that relieves a carrier of its obligations under the Act if money is not provided to offset the cost of compliance. Furthermore, a "safe harbor" provision holds a carrier blameless if it deploys a technical solution to meet law enforcement's requirements that has been approved by a government-industry group, an industry trade group, or a standard setting authority capable of meeting law enforcement's capability requirements under Section 103 of the Act.

The Attorney General has delegated much of the responsibility for implementing the Act to the FBI. To facilitate implementation, the Director of the FBI has created the Telecommunication Industry Liaison Unit (TILU) made up of 70 to 80 persons and specialists to coordinate the efforts of the federal, state, and local law enforcement agencies in collaborating with the industry. TILU is intended to be a one-stop point of contact for all matters dealing with compliance with the Act.

---

[12] Section 301 of the Act added Section 229 to the Communications Act of 1934 by directing the FCC to convene a federal-state joint board to recommend appropriate changes to the FCC's separations rules. Regulated carriers will seek to recover costs through rate adjustments at the state level, and unregulated carriers will likely pass the costs to the customers.

[13] Testimony of Louis J. Freeh, Director, Federal Bureau of Investigation, before the U.S. Senate, Committee on the Judiciary, Subcommittee on Technology and the Law, and the U.S. House of Representatives, Committee on the Judiciary, Subcommittee on Civil and Constitutional Rights, Mar. 18, 1994, 103d Cong., 2d sess.

[14] The FBI's "Requirements" Document is in its fourth revision. The second revision was June 1994 (at that time it outlined nine requirements), the third revision (rev. 2.1), made Dec. 6, 1994, keyed the Law Enforcement's requirements to the organization of the 1994 Act, and combined the nine requirements into four in order to parallel the organization of the Act. The most recent revision was issued in May 1995.

Technical matters, cost reimbursement, compliance with capabilities and capacity, liaison with service providers and switch manufacturers/vendors, etc., are to be coordinated through this unit.

Even before the Act was passed, the law enforcement agencies and the industry had begun a collaborative effort to confront the problems of electronic surveillance. Building on earlier consultation with the industry through an informal industry technical working group that was convened more than two years before passage of the Act, a more formal arrangement was struck, which currently serves as the primary focus of government/industry collaboration.

In March 1993, the Electronic Communications Service Provider (ECSP) Committee was formed under the aegis of the Alliance for Telecommunications Industry Solutions (ATIS), an industry group aimed at resolving issues involving telecommunications standards and the development of operational guidelines.[15] The ECSP committee is co-chaired by an industry official and a representative of the Attorney General who represents the collective views of federal, state, and local law enforcement agencies.

ECSP is an open forum with over 200 individual participants (however, only 40 to 60 persons have consistently participated in the action teams), consisting of representatives of local exchange carriers, interexchange carriers, trade associations, industry consultants, equipment manufacturers, and law enforcement officials, among others.[16] Each participant must sign a nondisclosure agreement that is intended to both guard information that might be useful to the criminal element and to reduce the risk of divulging proprietary information, while ensuring a free and open forum for discussing mutual problems.

ECSP has created six action teams, each co-chaired by a representative of the industry and a representative of the law enforcement agencies:

- *Advanced Intelligent Networks (AIN):* Addresses solutions to problems related to the next-generation telephone network now in the initial stages of deployment. AIN involves the deployment of software-controlled devices, including signaling systems, switches, computer processors, and databases. These functional units enable subscribers to independently configure services to meet their needs, and in doing so, create another layer of complexity for wiretapping.
- *Personal Communication Services (PCS):* Considers solutions to problems arising from development of the next generation of wireless communication with the possible future capability of spanning the world.
- *Prioritization and Technology Review:* Responsible for establishing the priorities in attacking the problems associated with the various communication technologies. The action team is also charged with identifying future emerging communication technologies and features that must be dealt with in the future.
- *Switch-Based Solutions:* Develops recommendations to meet the functional requirements for the central switch office-based solutions to meet law enforcement's requirements, including operational security.

---

[15] Alliance for Telecommunications Industry Solutions (ATIS), 1200 G Street, N.W., Suite 500, Washington, DC 20005. Other industry associations have also been instrumental in developing the working relationship between the law enforcement agencies and the industry, including United States Telephone Association (USTA), Telecommunications Industry Association (TIA), and the Cellular Telecommunications Industry Association (CTIA), and other industry standards-setting bodies.

[16] ECSP does not include all of the industry groups involved in compliance with the Act. Many accredited standards-setting organizations and other trade organizations will play a role meeting technical and operational compliance requirements. One example of this is the Telecommunications Security Association (TSA); an association of security officials from the service providers that are responsible for executing authorized wiretaps for their respective companies. Individuals from this organization are involved in the ECSP effort, however.

- *Interfaces:* Assesses the requirements for physical, messaging, operational, and procedural interfaces to meet the needs of the law enforcement agencies.
- *Cellular:* Considers cellular technologies in the context of law enforcement's intercept requirements.

The objective of the action teams is to explore the implications of meeting law enforcement's electronic surveillance requirements on the telecommunications networks. To assist them in their objectives, they are preparing a series of consensus documents to serve as references for industry standards-setting bodies, service providers, equipment manufacturers, and law enforcement agencies. These documents, which are to be produced by each action team, will generally include:

- Requirements and Capabilities Document,
- Interpretation of Requirements Document,
- Features and Description Document, and
- User Performance Document.

Industry standards groups will use these documents to develop standards specifications that will guide manufacturers in the development and production of switches and other devices needed to meet the requirements of the law enforcement agencies.

LAW ENFORCEMENT'S REQUIREMENTS FOR ELECTRONIC SURVEILLANCE[17]

The requirements of the law enforcement agencies apply to *all* forms of electronic communications service providers. The requirements are, however, generally couched in terms that apply primarily to telephone communication. Nonetheless, the same requirements apply to any industry sector that provides common carriage of communications for sale, including the cable television industry, public utilities, and other forms of electronic communication, except information service providers, which are expressly exempted under the act.

These requirements, though stated in legal or descriptive terms based on Section 103 of the Act, when translated by engineers and service personnel into technical requirements, impose stringent and substantial challenges to equipment manufacturers and the service providers for meeting law enforcement's needs.

Communications Access

Each service provider is required to have procedures capable of activating and deactivating wiretaps within 24 hours after receiving a lawful intercept request. Law enforcement agencies may also require expeditious access to technical resources or assistance in activating the intercept or to obtain needed service information. In "emergency situations," (e.g., in cases where rapid response is required to eliminate threats to life, property, or national security) law enforcement agencies require access to the intercept subject's communication, and technical assistance within a few hours.

Law enforcement agencies require access to all electronic communications transmitted and received by an intercept subject. Access must be provided from anywhere within the service area of a service provider. Access to all call setup information necessary to identify the calling and called numbers, e.g., originating line number identification, and terminating line number identification for all completed and attempted calls, as well as access to the call content is required. Under this requirement, the carrier remains in custody of the call service, with the carrier's security personnel activating or deactivating an intercept only when presented with legal authority by a law enforcement agency. Law enforcement agencies require that the service providers have a 24-hour-

[17] This section of the report relies heavily on the material contained in the document "Law Enforcement's Requirements for Electronic Surveillance," May 1995 revision, pp. 2-14, Federal Bureau of Investigation, Washington, D.C. It should be noted that these requirements represent the law enforcement agencies' interpretation of the requirements under the Act. Some service provider's disagree with some of the interpretations presented in the FBI requirements document cited above.

per-day capability of accessing and monitoring simultaneous calls originated or received by an intercept subject at the moment the call is taking place.

Law enforcement agencies require carriers to provide for implementing multiple simultaneous intercepts within a service provider's system, central office or area.[18] This requirement includes the ability for different law enforcement agencies to simultaneously monitor the same intercept subject while maintaining confidentiality among the agencies. Each carrier is required to support all requested authorized intercepts within its service area. To meet these requirements, service providers are required to have reserve intercept capacity available to meet unexpected demands, which are to be set forth by the Attorney General on or before October 25, 1995. Law enforcement agencies need to be able to access and monitor simultaneous calls placed or received by an intercept subject without the intercept being detected.

The service provider is only responsible for access as long as the call is under its control or maintains access to the call. If the original service provider does not maintain access to the ongoing call, it is that service provider's responsibility to provide any available information to law enforcement that identifies the visited service area and/or carrier. Once handed off to a second service provider, it is the second provider's responsibility to provide the access to law enforcement. The originating carrier, however, must notify the law enforcement agency to which carrier the call has been handed off.

Access is specifically required for call identifying information.

Call identifying information includes, for example:

- information concerning an intercept targets connection or transmission path to the network,[19]
- information concerning a calling party's connection or transmission path to the network when in contact with the intercept subject,
- dialing and signaling information generated by the intercept subject,
- directory numbers used in transferring or forwarding calls, and
- notification that a call or call attempt has occurred.

The nature and type of call setup information will vary depending on what type of communication service the calling or terminating party is using, i.e., information available from a call originated from a cellular phone will be different than if the call originated through a wired system. (See table 1-1.)

Dialing and Signaling Information

Law enforcement requires access to all dialing and signaling information for all calls originated by the intercept target, e.g., all digits dialed by the intercept subject and any information used to establish or direct call flow. In addition, after the call is completed (cut-through), law enforcement requires dialing information generated by the subject, e.g., touch-tone digits dialed to activate or code a device at the point of call termination.

Examples of dialing and signaling information include:

- All digits dialed by the subject and any signaling information used to establish or direct call flow, e.g., activating service features like call forwarding or three-way calling.
- Subsequent dialing information generated by the subject after cut-through (connection), e.g., dialed digits, voice dialing, etc.
- The terminating or destination number derived by the originating switch based on its interpretation of the subject's dialed digits or other call direction commands.

[18] The number of simultaneous intercepts that a particular switch or system can accommodate is referred to as "capacity."

[19] "Transmission path" refers to connection or link from a subscriber's terminal to the network. The path may be over a wireline or radio link.

TABLE 1-1: Type of Call Setup Information Required for Common Telecommunication Services

Calling Party's Line Information	Service Type	Intercept Subject's Line Information
■ Directory Number	Plain Old Telephone Service (POTS)	▪ Directory Number (DN)
▪ Associated Directory Number ▪ Line Equipment Identifier ▪ Call Type/Bearer Capability ▪ Service Profile Identifier (SPID)	Integrated Services Digital Network (ISDN)	▪ Associated Directory Number ▪ Line Equipment Identifier ▪ Call Type/Bearer Capability ▪ Service Profile Identifier
▪ Numbers used by the service provider switch to identify the PBX and the caller behind the PBX —Directory Number of the PBX —Station identifier of the calling party (if available)	Private Branch Exchange (PBX)	▪ Numbers use by the service provider switch to identify the PBX and the caller behind the PBX —Directory Number of the PBX —Station identifier of the called party (if available)
▪ Directory Number	Coin	▪ Directory Number
▪ Electronic Serial Number (ESN) ▪ Mobile Identification Number (M IN)	Cellular	▪ Electronic Serial Number (ESN) ▪ Mobile Identification Number (M IN)
▪ Personal Number/Directory Number ▪ Terminal Equipment Identifier	Personal Communications Services (PCS)	▪ Personal Number/Directory Number ▪ Terminal Equipment Identifier
▪ Directory Number	Other Special and Proprietary Customer Premises Equipment (CPE) Interfaces (Non-POTS or Non-ISDN Signaling)	▪ Directory Number ▪ Other available items, for example, Automatic Numbering Identification (ANI)

SOURCE Federal Bureau of Investigation.

Redirection Numbers

Access to call setup information includes redirection numbers when calls are forwarded or transferred using custom calling features, for example when multiple forwards or transfers are involved in a call attempt. A call initiated by a calling party to the intercept subject maybe forwarded or transferred several times before reaching the intercept target. In those cases, law enforcement requires the number of the party that originated the call, and any intermediate numbers used to redirect the call.[20] Access is required to forwarded-to numbers if control of the call remains with the service provider executing a lawful wiretap.

Call Attempt Alerts

Notification of all call attempts placed by or to the intercept target are required. Currently, in the case of wireline communications intercepted in a local exchange carrier's (LEC) service area, law enforcement agencies generate a time stamp after automatically detecting signals for ringing, or when a receiver is taken off or placed back on its hook. New technologies will make the simple detection

20 According to industry representatives participating in the ECSP, current network signaling can provide the Original calling number, the original called number, and the last redirected number. It is not considered to be technologically feasible with existing standards for interswitch signaling to provide more than this unless the entire signaling system is changing to provide these capabilities.

methods more difficult as out-of-band (i.e., off-line) signaling using computer-controlled signal transfer points replaces conventional in-band (on-line) signaling systems commonly used by many local exchange carriers today. Therefore, law enforcement agencies will require some form of notification from the carrier so that monitoring equipment can be activated.

Call Content

Law enforcement agencies must have access to the contents[21] of calls placed or received by intercept subjects. In some modes of transmission, the electronic communication may be carried on two different channels (duplex), with one party on one channel, and the other on a second channel. Nonetheless, the carriers must provide uninterrupted access to both channels simultaneously.

There are three possible combinations for placing and receiving calls:

- wireline-to-wireline, including Plain Old Telephone Service (POTS), coin operated service, and Integrated Service Digital Network (ISDN);
- wireline-to-mobile or mobile-to-wireline, where one party uses a cellular, PCS service or other wireless service, and the second party uses a wireline service; and
- mobile-to-mobile services, where both parties use cellular, PCS service or other wireless service (See figure 1-4.)

Custom calling features allow subscribers to forward or redirect their calls, or set up conference calls involving more than two parties. In these cases, a service provider is required to provide access to the call so long as it maintains access to the communications. If a call from an intercept target is redirected so that the authorized service provider loses access to the call, the provider must notify the law enforcement agency of the identity of the service provider who then has custody of the intercept call. If the new service provider's identity is not known, the carrier must provide any supplemental information that would assist the law enforcement agency in determining the new service provider's identity.

Mobile Communications

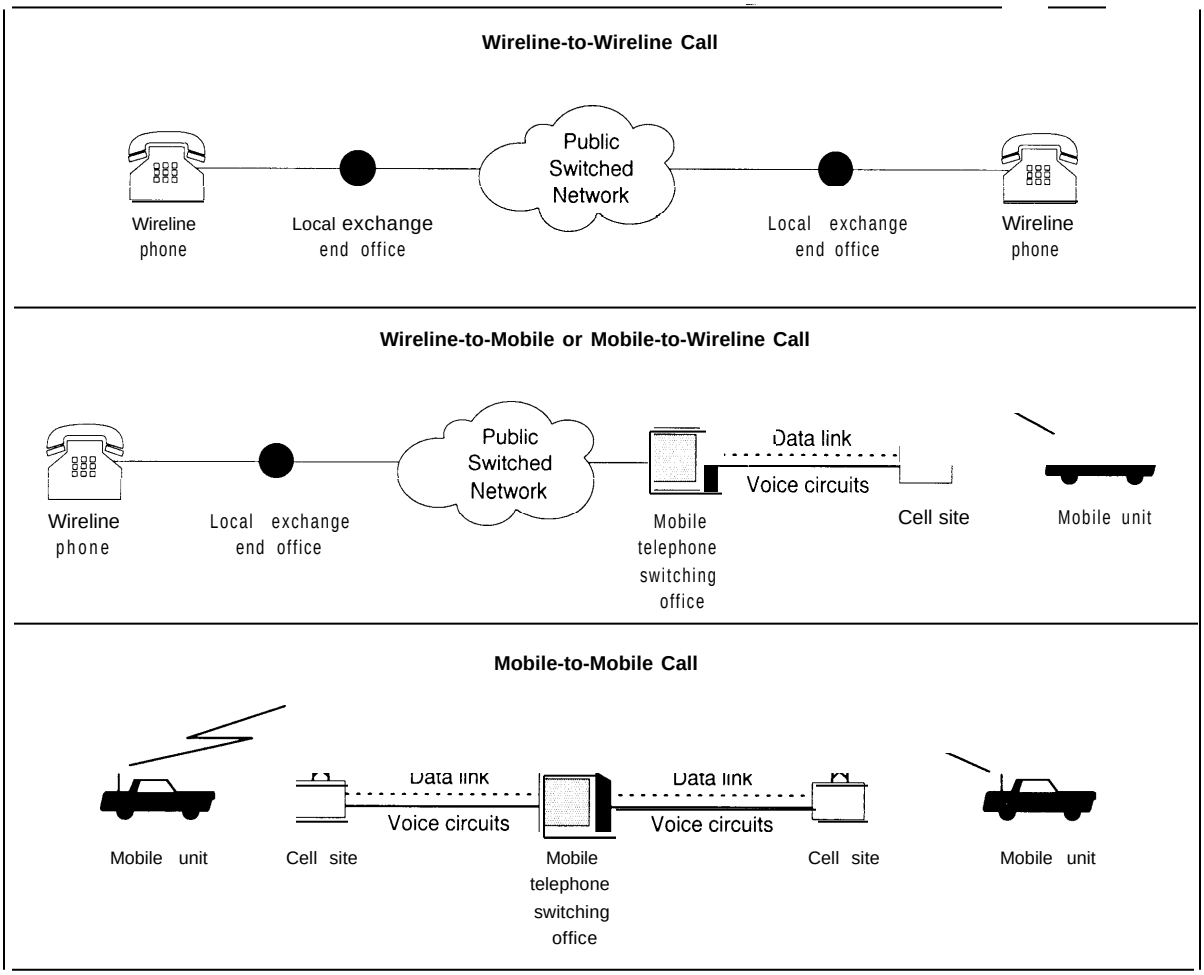
Requirements for accessing call setup information and call content apply to both wireline and wireless mobile communications. A mobile customer can move freely about a home service area and beyond into the service area of another mobile carrier. A service provider's network may cover a local area, a region, a state, or portions of a multistate area. When a single service provider covers a large geographic area, that carrier is required to provide access to an intercept subject's communication wherever it takes place within the provider's extended service area consistent with the court order authorizing the intercept. Law enforcement agencies require access to an intercept subject's communications throughout the area served by his or her home service provider. When an intercept subject travels into another service provider's area while communicating, law enforcement agencies require access to the ongoing call so long as the home service provider maintains access to the call in progress. If access to the call is not maintained by the home service provider, law enforcement agencies require that the identity of the service provider to which the call was handed off be made available, or that information be provided that will enable the new service provider to be identified. (See figure 1-5.)

The discussion above focused on the case where a mobile intercept subject originated a call in his or her home service provider area and traveled to an adjacent service provider's area in the course of a call, and the call is handed off to another service provider.

Subscribers who "roam" beyond their home service provider's area and attempt to establish communication from another service provider's

[21] "Call content" refers to any type of electronic communications sent by or sent to the intercept subject, including transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature.

FIGURE 1-4: Examples of Possible Communication Links Among Wireline and Mobile Services



SOURCE Federal Bureau of Investigation, 1994

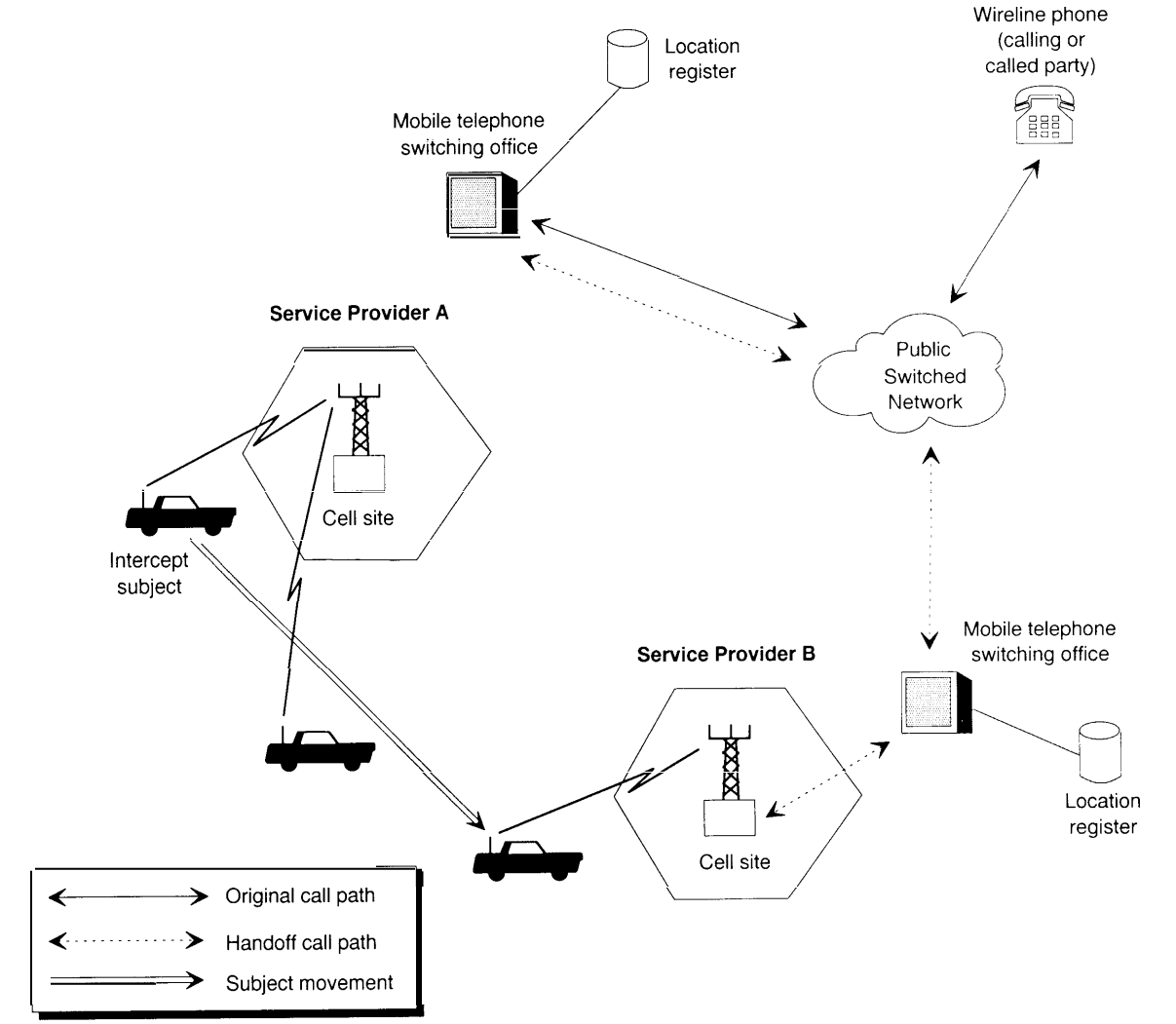
area are registered as visitors in the new service. In those instances, information about the caller's unique Electronic Serial Number (ESN) and Mobile Identification Number (MIN) and other authentication, validation, and routing information are automatically exchanged between the location registers (computer databanks) of the two cellular service providers. (See figure 1-6.)

Law enforcement agencies require access to information regarding the identity of service providers that request visitor's registration authorization from an intercept subject's home service provider. The home service provider must provide the law enforcement agencies with the visited service provider's identity, and other data, such as service site information of the carrier that is controlling the intercept subject's communication.

■ Delivery of Information to Law Enforcement

Law enforcement agencies require that call content and call setup information that is intercepted in response to an authorized wiretap be trans-

FIGURE 1-5: Mobile Intercept Subject Travels from Home Service Provider to an Adjacent Service Provider (home service provider retains access to the cell)

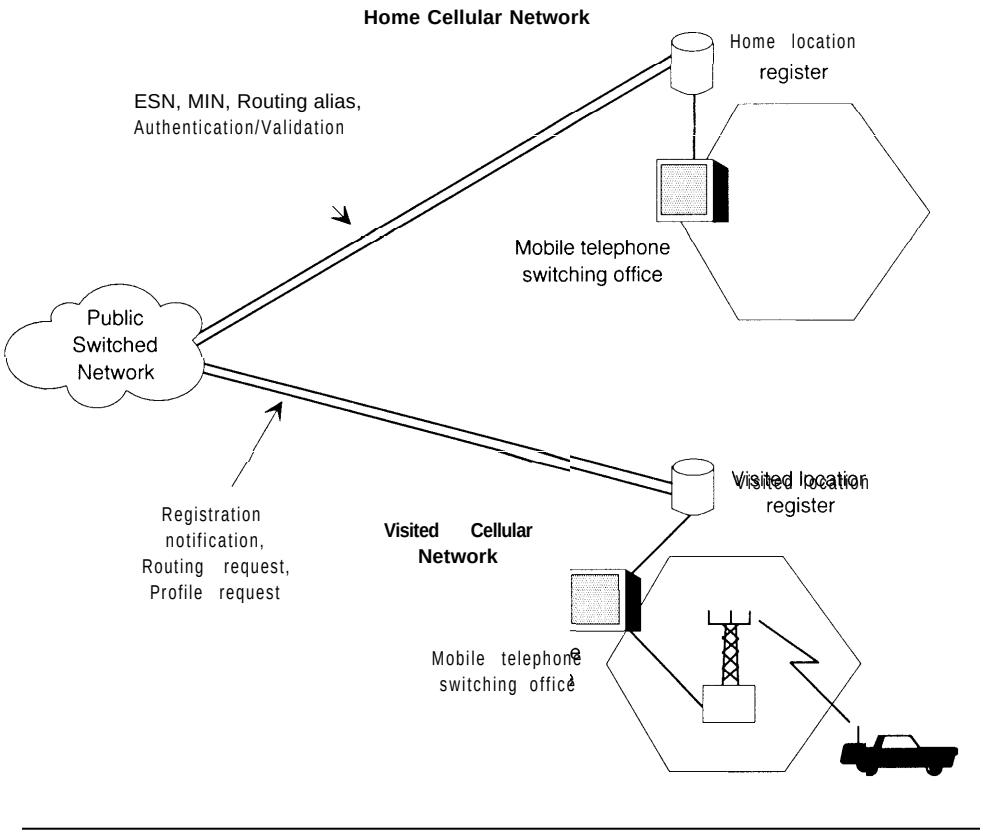


SOURCE Federal Bureau of Investigation, 1994.

mitted to a designated law enforcement monitoring facility. However, access to the intercept will be controlled by the service provider and not the law enforcement agency. Transmission of intercepted communications must satisfy the following guidelines:

- Where call setup information and call content are separated during interception, the service provider must take steps to ensure accurate association of call setup information with call content.
- Transmission of the intercepted communication to the monitoring site must be made without altering the call content or meaning.
- Law enforcement agencies require that the transmission facilities and formats of the information transmitted the monitoring stations be in a standard form.

FIGURE 1-6: Registration Information Exchange During Roaming



SOURCE Federal Bureau of Investigation, 1994

- If the service provider controls and/or provides coding, compression, encryption, or other security features for the intercepted communications, the service provider must decode, decompress, or decrypt intercepted messages before transmission or provide the capabilities to the law enforcement agency to reprocess the information.
- Law enforcement agencies require that the service provider use a minimum number of transmission facilities to deliver the intercepted communications to the monitoring facility. Currently, most cellular service areas with multiple Mobile Switching Centers (MSC) require a connection from each MSC to the monitoring location for each intercepted call.

■ Verification Information

Law enforcement agencies require that the carrier provide information to verify or authenticate the linkage between the intercepted communications and the intercept subject in order to establish the wiretap as evidence in court, however, it is law enforcement's responsibility to authenticate the linkage. Prior to implementation of the intercept, the service provider is obligated to provide the law enforcement agency with information on the services and features subscribed to by the intercept subject (service profile).

Courts require law enforcement agencies to verify that the communication that was monitored was that of the intercept subject authorized in the

lawful authorization of the wiretap. This is done with a network identifier (directory number), terminal identifier, personal identification number, and billing and caller identification-related information.

Service profile information, i.e., the service subscribed to by an intercept subject, must be made available to a law enforcement agency in response to a lawful inquiry before and during an intercept. Service providers are obligated to notify the law enforcement agency of changes in the intercept subject's service profile during the progress of an interception, even if the change is initiated directly by the intercept subject without the involvement of the service provider, e.g., call forwarding.

Reliability of Service

Reliability of service for intercepted communications delivered to a law enforcement agency must be of equal reliability as that of the intercept subject's service. Service providers must also have the ability to detect and solve problems with the interception of call setup information or content information, as well as the transmission of the intercepted information to the law enforcement monitoring facility.

Quality of Service

The quality of the service supporting the intercept must be at least equal to the quality of the service provided to the intercept subject, measured by any objective factor, e.g., signal-to-noise ratio, bit error rate, or other parameters that measure transmission quality.

Transparency of Interceptions

Intercepts must be undetectable by the intercept subject or other callers, and known only to the monitoring law enforcement agency and authorized personnel of the service provider responsible for setting up the intercept. In some cases, intercept subjects may use sophisticated equipment to detect intercepts; nonetheless, service providers are obligated only to provide transparency within the limits of their equipment based on industry standards for transmission characteristics. Benchmarks for meeting the transparency requirement include:

- The subject should not be able to discern that an intercept is in progress.
- If the intercept begins during a call in progress, the intercept should not disrupt or interrupt the ongoing call.
- If in the process of interception, changes in services or features occur, these changes should not be apparent to the intercept subject or other parties
- Any line noise introduced by the intercept should not be perceptible to the intercept subject or other parties.

Network and Intercept Security

Service providers are also required to adopt operating procedures that safeguard against unauthorized or improper intercept and to prevent compromise of transparency. Such procedures include:

- internal restrictions on information about intercepts,
- security mechanisms for activating and deactivating intercepts,
- physical security to limit access to systems supporting intercepts,
- procedures to prevent disclosure of service changes caused by implementation of intercepts, and
- restrictions on knowledge of the existence of intercepts among service provider's employees.

Network security and integrity is addressed in Section 105 of the Act.[22] The Act directs that only an employee of a service provider can activate an intercept after the receipt of a lawful authorization from a law enforcement agency, according to procedures prescribed by the Federal Communica-

[22] Section 301 of the Act also directs the FCC to establish rules to implement Sec. 105.

tion Commission (FCC). (Sec. 229(b)) However, other security matters not addressed by the Act figure prominently in maintaining network security protecting the integrity of electronic surveillance.

Computer systems, in general, are susceptible to breaches of security under the most strict controls. This is evident from the violation of even relatively secure computer systems and networks within the Department of Defense. The modern telephone network is little more than an extension of a series of interconnected wide-area computer networks linked by transmission facilities. As such, telephone systems suffer the same vulnerabilities as all networked computer systems.[23] Whether or not the network may become more vulnerable as a consequence of meeting law enforcement's intercept requirements under the Act is uncertain. There is no empirical evidence that suggests that it will at this time.

The complexity of sophisticated computer systems is their source of vulnerability. Millions of lines of computer code are needed to operate a large networked computer system. The magnitude of the operating system creates hundreds of potential opportunities or windows for penetrating the system. On the other hand, a proficient person intent on hacking into the system need only find one of these windows to achieve his or her objective.

Maintaining a secure operational environment in the administration of electronic intercepts is a major concern in wiretap procedures. Security problems exist whether the intercept involves switched landlines, mobile cellular operations, or personal communication services. Security protocols are needed to prevent unauthorized personnel from: Initiating or terminating surveillance; obtaining information about a surveillance in progress; monitoring the results of a surveillance; determining past surveillance activities or acquiring information about the total number of activities or intercepts on a particular switch; and obtaining intelligence information from analysis of billing records and other business data.

Threats to security originate from both internal and external sources. Operational components and connections between the components involved in managing the setup and control of surveillance activities are particularly susceptible to intrusion. Telephone companies have been favorite victims of "hackers" since telecommunication networks became "computerized." Abuses by hackers have been aimed at switch elements, support billing, and other record-keeping functions.

Notwithstanding the concern for potential outside hackers, the internal security threats from intentional or careless breaches in security by telephone company employees, or contractors to service providers, may be a greater threat.

There are several categories of security risks:

- *Disclosure of Information*: Information about a specific surveillance may be obtained by an unauthorized individual, e.g., that a wiretap is being initiated on a specific target, or information gathered from the wiretap, might be made available to an outside individual. Even operational information about the number of surveillances performed at a single switch or within a service provider's area is considered to be sensitive information.
- *Redirection of Information*: There is a risk that intercepted information might be accidentally sent to the wrong location, or that it might intentionally be diverted to another location, or destroyed.
- *Manipulation of Information*: Data transmitted to and received by law enforcement officials must be reliable. No doubt about its association with the intercept target and the integrity of the

[23] The recent arrest of Kevin D. Mitnick, a well-known and previously convicted computer hacker, for computer crimes, points to the problem confronting computer and telephone networks at the hands of talented and skillful computer criminals. It is alleged that Mr. Mitnick broke into computer networks and stole files and acquired 20,000 credit-card numbers by tampering with a telephone switch in a cellular service provider to reroute his calls to evade surveillance. John Markoff, *New York Times*, p. 1, Thursday, Feb. 16, 1995, John Schwartz, *Washington Post*, Sunday, Feb. 19, 1995, p. 1.

information can exist if it is to be accepted as evidence by the Courts. Neither intentional nor unintentional manipulation or corruption of the data must occur.

- *Destruction of Information*: Information used to control the establishment of surveillance could be lost or destroyed, resulting in failure to perform the surveillance.
- *Internal Risks from Trusted Personnel*: Fraudulent initiation or termination of intercepts, or disclosure of intercept information.

There are physical ways to protect the integrity of electronic intercepts, and ways in which databases and records can be protected from tampering (logical means of protection). Physical protection includes:

- control of information to initiate a wiretap to prevent unauthorized disclosure;
- restricted access at the service provider's facility; and
- physical security in the transmission system and control points outside the carrier's plant to prevent unauthorized interceptions.

Logical approaches to protection of data and records include:

- partitioning databases, switch function, peripherals, etc.;
- auditing systems to secure the storage and processing of business records provided to law enforcement agencies in the course of an intercept;
- controlling access through logging procedures for entry into the operational components controlling the intercept;
- prohibiting direct remote access through dial-in procedures to an operational component involved in an intercept; and
- encryption of data transmitted to the law enforcement monitoring site to prevent access to the intercepted information in the course of its transmission from the distribution point to the law enforcement monitoring site.

FINDINGS AND OBSERVATIONS

The Communications Assistance for Law Enforcement Act was approved on October 25, 1994. The act is currently in an early stage of organization, planning, and implementation. Few conclusions can be reached on a cursory examination of the progress made over the short period of observation. Nevertheless, a few indicators are worth noting:

- ***General Observation*: Although the technical complexity of modifying the existing network and designing features into new technology that will meet law enforcement's electronic surveillance needs is not trivial, the industry is highly competent and capable of meeting the technical challenges. If major problems arise in meeting the needs of law enforcement, they will likely arise as a result of institutional difficulties in dealing with a diverse, highly entrepreneurial industry made up of a large number of telecommunications companies offering many new innovations and features, with the number of players steadily increasing.**
- ***Timing:* There is a possibility that the complexity of re-engineering and modifying the technology installed in the current telephone network to meet Law Enforcement's needs may exceed the time allowed for compliance by the Act.**

The Attorney General is to notify the carriers of the "actual and "maximum" capacities by October 25, 1995 required to meet law enforcement's requirements to bring the carrier's technology up to specifications. The carriers must then respond to the Attorney General's notification with statements of their ability to meet the capacity and capability requirements within 180 days. Carriers then have three additional years (four years after approval of the Act) to comply with law enforcement's requirements (October 25, 1998).

If the Attorney General fails to meet the October 25, 1995 deadline for publishing Law Enforcement's capacity notice, then the service provider's compliance will be delayed accordingly. If the carriers decide that law enforcement's requirements are not reasonably achievable within the allotted time, they can petition the FCC for an extension of up to two years. This would push back the required compliance date to as late as October 25, 2000.

There remains a question as to whether there will be sufficient time for publishing law enforcement's capacity requirements, completing the ongoing consultative process between the industry and Law Enforcement, providing accredited standards bodies with specific input needed to meet Law Enforcement's requirements, completing the process leading to accepted industry standards or collaborative solutions as well as allowing time for switch manufacturers to engineer and develop the modifications, and manufacturing, delivering, installing, and debugging the switch modifications.

Once a clear set of generic specifications is available, it generally requires two years to develop the software and hardware to implement a complex set of new features. Simple modifications may require less time. Adjustment and debugging of supporting software and operating procedures, including revising security procedures within the carrier's operations, may require considerable time and involve a high level of uncertainty.

The above holds true only for conventional telephone switches in the service provider's central office. Advanced Intelligent Networks (AIN), which operate interactively with software-based computer systems present more complex problems and a higher level of uncertainty about the seamless operation without service interruption. As with any software modification, those for AIN systems are complex, sometimes tricky, and in the worst case, can bring down a network if there is a malfunction (malfunctions of this nature are not specific to AIN, but their complexity makes them more vulnerable).

Cellular systems present complex operational problems to handle all hand-offs to other carriers, etc. New modes of transmission, e.g., PCS, provision of telephone service by cable television companies, and Asynchronous Transfer Mode (ATM) fast-packet networks are future technologies that will allow time for further development without hindering Law Enforcement's mission.

- ***Security:*** **The installation of technologies to meet law enforcement's requirements will place new demands on carriers to ensure the security of the intercepted information and of the network at large.**

Security of the telephone system is a more serious problem than news accounts suggest. There is a concerted effort by the telephone companies to play down security breaches, but many more have occurred than the public is aware. Anecdotal evidence in the possession of the carriers indicate that communication networks (even the Department of Defense) have frequently been penetrated by hackers. By using debug routines and "spoofed" passwords (to mimic those with legitimate privileges) hackers have been able to extract passwords and personal identification numbers, to make fraudulent calls and illegal transactions. Others have maliciously altered databases or extracted personal information that they were not authorized to have. Allegedly, there is a black market for surveillance, where clever hackers can establish surveillance of individuals from outside the system. Though publicly unconfirmed, there have been accounts of suspected incidents where hackers have even intercepted law enforcement communications, including the contents of wiretaps, although it is highly unlikely that this has occurred given the complexity of taking such action. In other instances, intercepts may have been disconnected from the outside through software switches. It is also possible for hackers to determine who is being tapped, which could be of value to the criminal element.

Not all of the security problems originate from the outside. There have been occasions where tele-

phone personnel, or manufacturers/vendors technicians, who know the system and have access from the inside, are motivated to make fraudulent use of information obtainable from computer-based databanks.

The security requirements of P.L. 103-414 will require the industry to tighten its supervision over information regarding the existence of a wiretap and the identification of those who are tapped. Furthermore, the content of the intercepted calls will require protection, since law enforcement listening (monitoring) posts may be some distance from the tapped switch (linked by leased or private lines), with opportunities for others to modify or obscure the contents or otherwise diminish its integrity as evidence.

- ***Safe Harbor*: The government may have to make an affirmative declaration that an "adopted" industry standard or technical requirement is sufficient to satisfy the "safe harbor" provisions of the Act.**

Section 107(a) of the Act provides that if equipment to meet law enforcement's requirements is built to meet "publicly available technical requirements or standards adopted by an industry association or standard-setting organization," vendors or service providers will be considered in compliance with the Act if the standard or technical requirements meet the requirements of Section 103 of the Act. If standards are accepted by an accredited standards-setting organization, the clear meaning of the Act would protect carriers and vendors from charges of noncompliance. However, the Act is ambiguous with regard to what constitutes "adopted by an industry association." Standards certified by an accredited standards organization go through formal processes and orderly steps of approval before being certified as a standard. "Industry associations," without standards-setting functions, on the other hand, may have no formal approval process and operate loosely by consensus only.

The Electronic Communication Service Providers Committee (ECSP) is the primary industry-wide body that has dealt with the requirements of the Act. ECSP is sponsored and provided administrative support by the Alliance for Telecommunications Industry Solutions (ATIS). The ECSP is not an accredited standards setting body as generally recognized. However, ATIS does sponsor other recognized standards setting bodies (T1, Protection Engineers Group (PEG), Standards Committee 05, etc.). Within the ECSP, only the Cellular Action Team and the Personal Communication Action Team are coordinating their work on electronic intercept solutions through accredited standards organizations.[24]

The ECSP committee, however, is only one of many possible industry groups with the expertise to develop technical requirements. Any industry organization that tackles the task would be expected to include the involvement of the of the FBI's Telecommunications Industry Liaison Unit (TILU) in its deliberations to ensure that its standards meet the capability requirements of Section 103 of the Act.

Whether a general consensus reached by ECSP participants or any other industry organization on technical requirements would constitute "adopted by the industry" in meeting the requirements of the Act is unclear. Industry participants in ECSP have raised questions regarding the official status of the work produced by the Committee. Thus far, the government has not responded to industry's concerns in a definitive way.

If the industry fails to issue technical requirements or standards, or if it is believed that the technical requirements are deficient, the FCC is empowered to establish such requirements or standards if petitioned to do so by any person or entity. This process could be used by anyone, including law enforcement agencies, to petition the FCC to establish an adequate standard.

[24] The Standards Organization for Cellular Technologies is designated TR45. TR46 covers PCS technologies. Both standards groups operate under the aegis of the Telephone Industry Association (TIA).

Continued uncertainty about what constitutes an "adopted" industry technical requirement could result in future litigation to decide the question should a cause of action arise. To avoid the prospect of future litigation and possible delays, the government might consider a certification process for standards or technical requirements that would assure the industry that a technical requirement that is developed by consent of a non-standards-setting association would provide them with a safe harbor from sanctions for noncompliance.

One option might be to use the authority provided the FCC for establishing standards under Section 107(b). Association-approved technical requirements (absent an accredited standard) could be referred to the FCC for evaluation and formal adoption.

- ***Cost Reimbursement:*** **If the Act is to achieve its intent with regard to upgrading law enforcement's ability to intercept electronic communications in the existing network (equipment installed prior to January 1, 1995), then Congress must appropriate sufficient funds (and the Attorney General must make them available to the service providers) to offset the costs of retrofitting. Reliable cost data for detailed fiscal planning will likely not be available until the budget period for fiscal year 1996.**

Reliable engineering and operational cost estimates cannot be made until after the Attorney General issues the capacity requirements that the individual service providers must meet to comply with the Act. At the time of this report (spring 1995), there have been no decisions on the technology needed to meet the capabilities for electronic surveillance required by the law enforcement agencies. Furthermore, the capacity and specific geographical priorities for implementing the Act are not scheduled for release until fall of 1995.

Failure of the government to appropriate and expend adequate funds to pay the carrier's expenses for complying with the act will automatically place the carriers in legal compliance with the act (for equipment installed prior to 1995), but would not result in the deployment of the technology needed by the law enforcement community in the timeframe set forth in the Act.

In the event that sufficient funds are not appropriated for the purpose of offsetting the costs to carriers for retrofitting pre-1995 equipment, the rate of replacement of existing equipment with new equipment that would be required to meet law enforcement's capability requirements would depend on the business plans of the individual service providers. Such plans could depend on market strategies, age and condition of the service providers equipment, development of new technologies, tax consequences, etc. This could result in spotty and uneven deployment of new equipment, with the capabilities and capacity to meet the Act's requirements (islands of capability), located among service areas of other providers that continue to operate old equipment that does not comply with law enforcement's requirements.

The General Accounting Office (GAO) is mandated by the Act to compile cost estimates in a report from the Comptroller General that is due April 1996 and every two years thereafter. The GAO report is to include "findings and conclusions. . .on the costs to be incurred by telecommunications carriers. . .including projections of the amounts expected to be incurred and a description of the equipment, facilities, or services for which they are expected to be incurred." (Sec. 112(b)(2)).

- ***Future Technologies:*** **Law enforcement agencies will continually face challenges in maintaining their electronic surveillance capabilities in the future as new communications technologies and services are developed.**

The field of communication technology is developing rapidly. A stream of new technologies are qued to complement, compete, or displace the communications systems of today. Computer-based packet communications systems, satellite-based global communications, and the interconnection of virtually every form of electronic communication system through a National In-

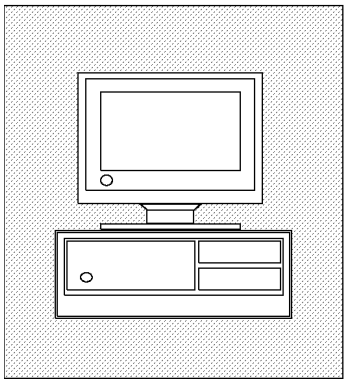
formation Infrastructure (NII) will require law enforcement agencies to keep abreast of these developments as they come online. Along with the technological challenges that future systems will bring, are institutional and international issues that must be addressed as global communication systems are developed.

Technical Aspects of Electronic Surveillance[1]

2

The evolution of the modern telephone system, from its invention in 1876 followed a predictable path of development until digital technology and optical fiber began seriously supplanting analog technology and copper wire in the U.S. telephone system. Since about the 1970s the technology of electronic switching, digital processing, computer architecture, and optical transmission have progressively developed into commercial devices and applications whose low costs and broad capabilities have made these technologies the foundation of a new era of communications.

The speed with which the nation's communication system is shifting from a wire-based analog system to digital computer-controlled switches and optical fiber is astounding. In 1989, nearly one-half of the major telephone companies' switches were digital. By 1993 the proportion of digital switches had grown to 80 percent.[2] Fiber optic transmission systems also are rapidly displacing copper in local service and long distance carriers. In 1985, long distance carriers had about 20,000 miles of fiber optic cable in service. By 1993 the long distance companies reported slightly



[1] Material in this chapter was synthesized from documents prepared by the various action teams of the Electronic Communication Service Providers (ECSP) committee, operating under the aegis of the Alliance for Telecommunications Industry Solutions (ASIS). The OTA project director for this report attended the functions of the ECSP under a nondisclosure agreement. The material herein contains no information considered to be sensitive by the law enforcement agencies, or proprietary by the industry personnel reviewing the draft document.

[2] Testimony of A. Richard Metzger, Jr., Deputy Chief, Common Carrier Bureau, Federal Communications Commission, before the U.S. House of Representatives, Committee on Energy and Commerce, Subcommittee on Telecommunications and Finance, Sept. 13, 1994, 103d Cong., 2d sess.

more than 99,000 miles of optical fiber.[3] Local telephone companies had about 17,000 miles of optical fiber installed in 1985, and this grew to over 225,000 miles by 1993.[4]

The recent explosion of wireless communication has extended mobile service to more than 734 metropolitan and rural service areas. These service areas geographically overlay the wired telecommunication systems to which they interconnect. Currently, there are over 1,100 cellular switches in operation in the United States.[5] The growth of wireless communication has been remarkable. Today, there are more than 16 million cellular subscribers, and the cellular industry estimates that subscribership will double by 1998.[6] Following behind is the next generation of wireless services, the new Personal Communication Services (PCS), which are similar in function to today's cellular communication services, but new PCS entrants may develop entirely new services in the future, which could present different problems to law enforcement agencies. Coming next will be satellite-based communications systems for personal communication that could extend wireless communication to nearly every quarter of the world.

In addition, a convergence of digital and analog technologies is bringing other nontraditional sectors of the communication industry into what once was the domain of the telephone companies. Government deregulation and industry restructuring has the potential for further blurring the business lines between the cable television industry and the telephone carriers, and has raised the prospect that electrical utilities might someday be competitors in the telecommunications market as well.[7]

Through the 1950s and into the 1970s law enforcement's wiretap requirements were easily met. The nation's telephone system largely consisted of twisted copper wires that connected subscribers to central office switches that routed the calls to their destinations through copper cables or overland via microwave radio, and later satellites. The transmitting and receiving instruments were commonly used telephones. Business may have had Private Branch Exchanges (PBX) to route their calls. But in general, it was a comparatively simple system of wires connected to switches that connected to other wires that routed the calls to businesses and residences. Law enforcement officials, armed with the necessary legal authorization, would simply physically connect "alligator clips" to wire terminals and monitor the contents of calls coming to and going from the telephone line authorized in the wiretap order. (See figure 2-1.) Since much of the system was under the control of American Telephone and Telegraph (AT&T), although GTE and other independent telephone companies operated as well, the national system was largely based on the same standards, operating protocol, and equipment design used by AT&T.

In the recent past, additional complexities were added to the system when transmission technologies for the copper-based analog system were developed to provide more bandwidth, and hence speed, to handle larger volumes of calls. A transmission mode referred to by its industry standards name, "T1," and a faster version "T3," which was originally developed for intrasystem high-speed trunking, became available for high-volume users, largely businesses.

---

[3] Federal Communications Commission, Fiber Deployment Update, table 1, May 1994.

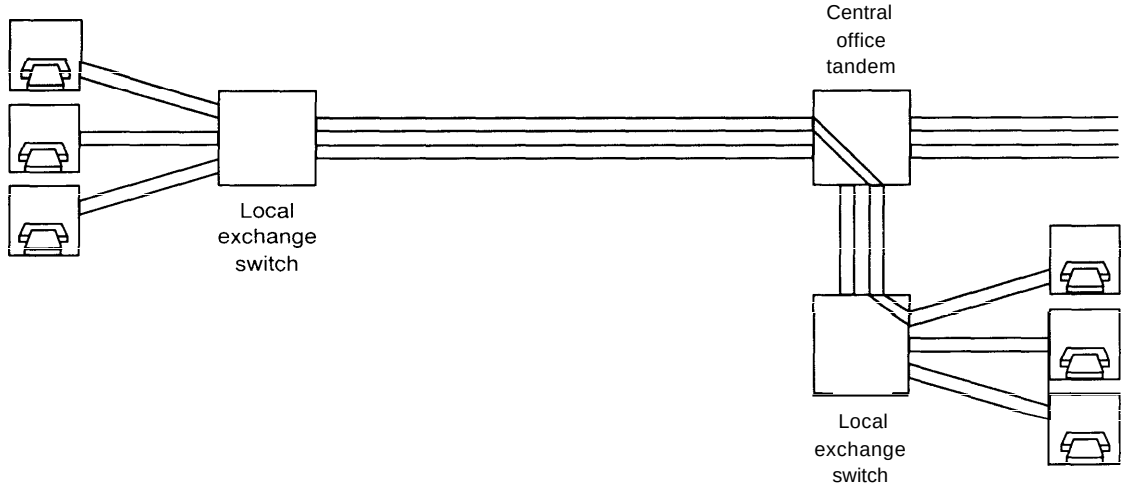
[4] Id at table 5.

[5] Testimony of Thomas W. Wheeler, President and CEO, Cellular Telecommunications Industry Association, before hearings of the U.S. House of Representatives, Committee on Energy and Commerce, Subcommittee on Telecommunications and Finance, Sept. 19, 1994.

[6] Cellular Telecommunications Industry Association, "The Wireless Factbook," p. 36, spring 1994.

[7] James Carlini, Telecom Services, "Utilities are Hungary for a Piece of the Action," *Network World*, p. 55, Sept. 19, 1994.

FIGURE 2-1: Copper-Based Wire Analog System Connecting Plain Old Telephones (Pots) Through a Central Office Tandem Switch



SOURCE Off Ice of Technology Assessment, 1995

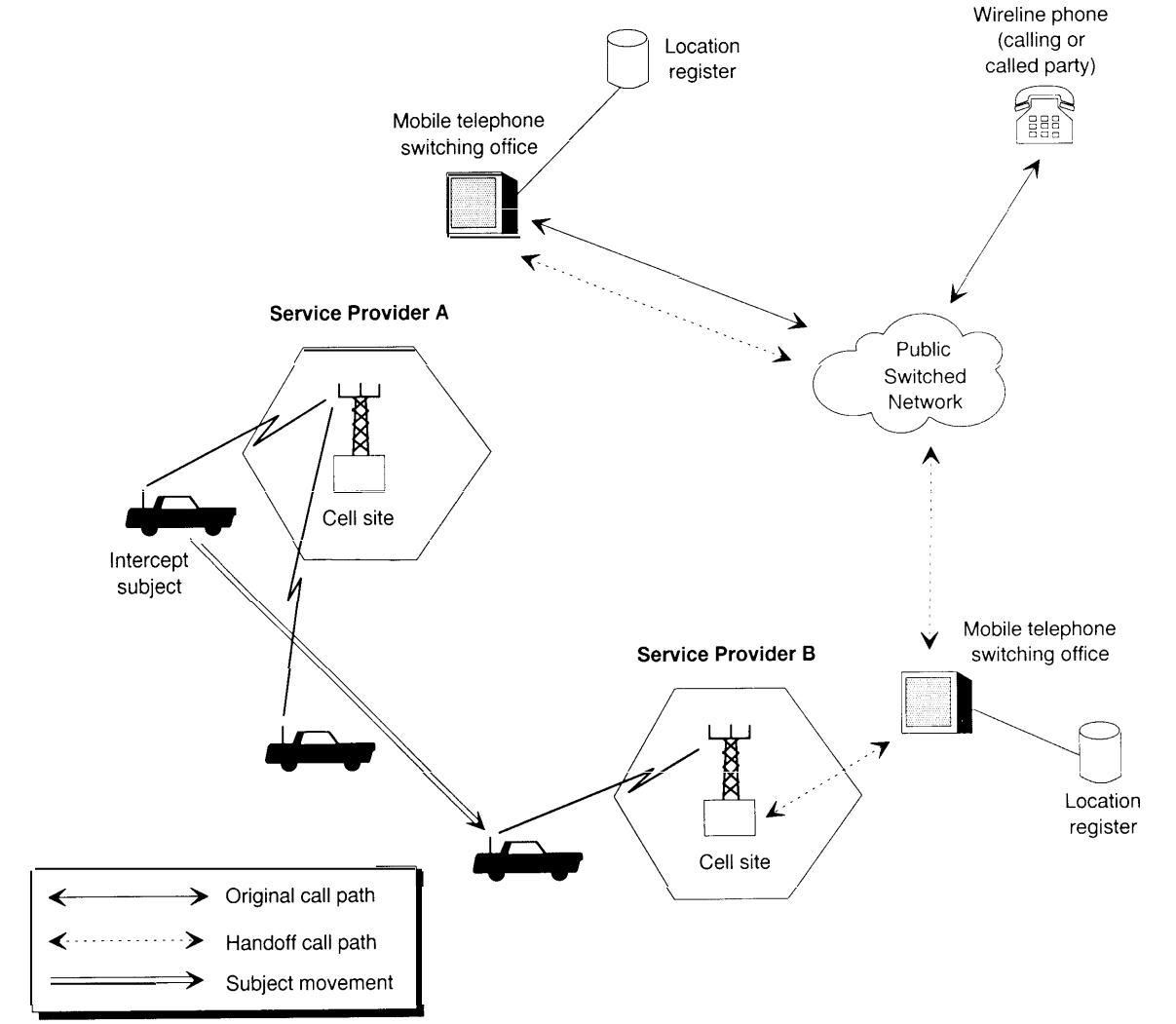
This technology gains its speed by separating the electronic signal into discrete segments divided sequentially in time (Time Division Multiplex, or TDM) and routing them sequentially over the line to be resequenced at the receiver (demultiplexed). In this way the signals are virtually routed over *channels so* that many more bits of information can be transmitted over the wire or coaxial cable at the same time.

Multiplexing can increase the normal speed of transmission from thousands of bits per second (kbs) to 1.544 million bits per second (Mbs) for T1 and 45 Mbs at the T3 rate. Because multiplexing breaks the continuity of the signal in the transmission phase, it places an additional degree of difficulty for electronic surveillance. Also, since 1984, long distance carriage has been separated from the local exchange carrier, so that now an intercepted call might flow among several different carriers on its way to or from a target. (See figure 2-2.)

The current telecommunication environment is considerably more complex. Wireless technology has expanded the reach of the telephone system. The combination of digital transmission, imbedded computer databases, digital switching, and the increased speed of optical fiber cables provide many more functions, options, and flexibility. As a result, many of the functions and operations, which were once the sole province of the telephone operating companies, are now performed directly by the subscriber, sometimes without the knowledge and control of the carrier. Wide-area centrex operations, for instance, allow a large business subscriber to manage a communication system within the carriers network, but independent of the carrier with regard to assigning internal number, call routing, and location identification-a virtual network within the carrier's network. Wireless subscribers may roam outside their home service area. Features such as call forwarding, speed dialing, call transfer, and specialized high-speed computer-based services add complexity to the problems of wiretapping for law enforcement agencies. (See figure 2-3.)

The future operating environment will contain several additional actors than are now present in the telecommunication network. Personal communication service providers (PCS) will extend the reach of wireless communication adding more

FIGURE 1-5: Mobile Intercept Subject Travels from Home Service Provider to an Adjacent Service Provider (home service provider retains access to the cell)

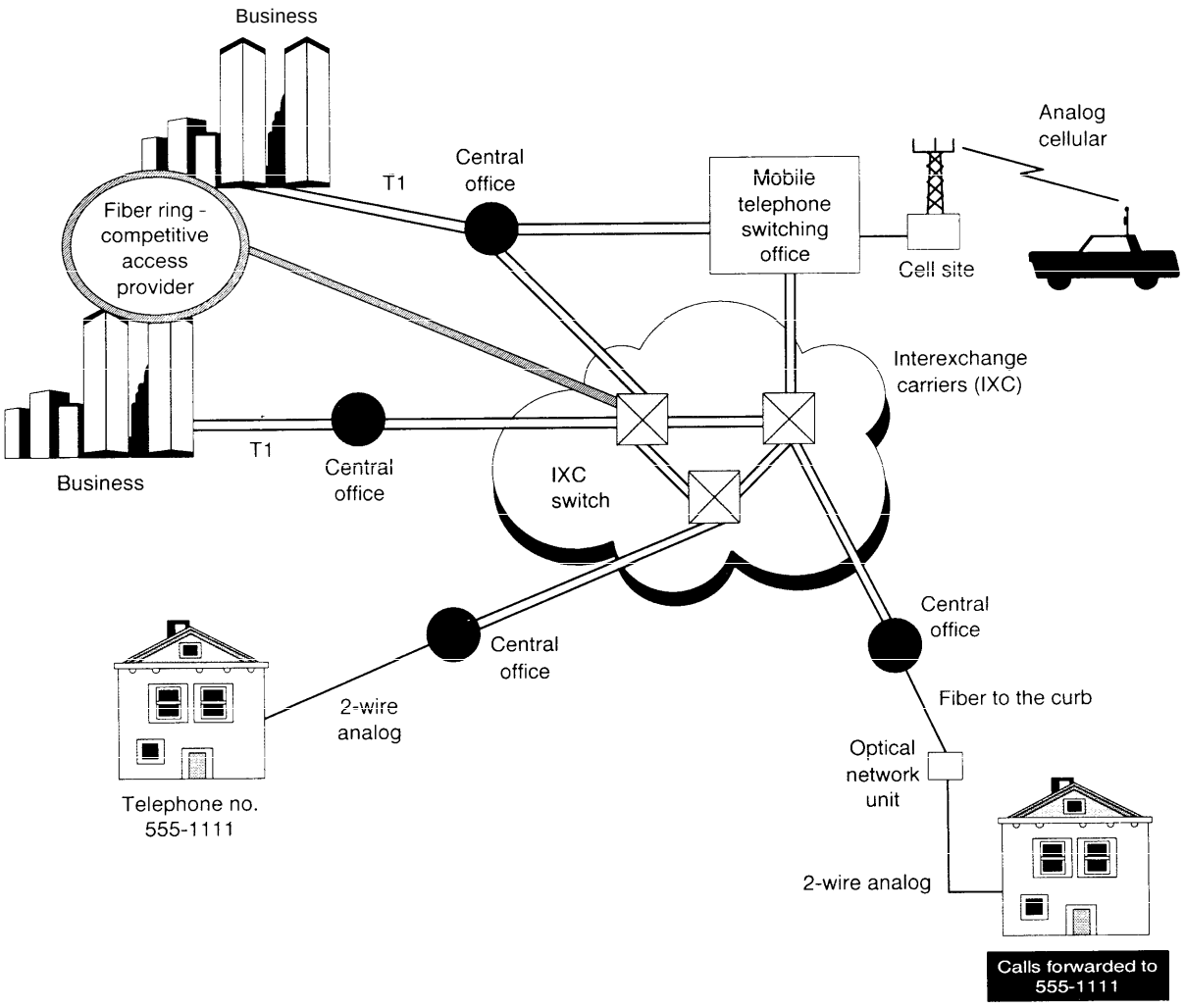


SOURCE Federal Bureau of Investigation, 1994.

mitted to a designated law enforcement monitoring facility. However, access to the intercept will be controlled by the service provider and not the law enforcement agency. Transmission of intercepted communications must satisfy the following guidelines:

- Where call setup information and call content are separated during interception, the service provider must take steps to ensure accurate association of call setup information with call content.
- Transmission of the intercepted communication to the monitoring site must be made without altering the call content or meaning.
- Law enforcement agencies require that the transmission facilities and formats of the information transmitted the monitoring stations be in a standard form.

FIGURE 2-3: Present Operating Environment



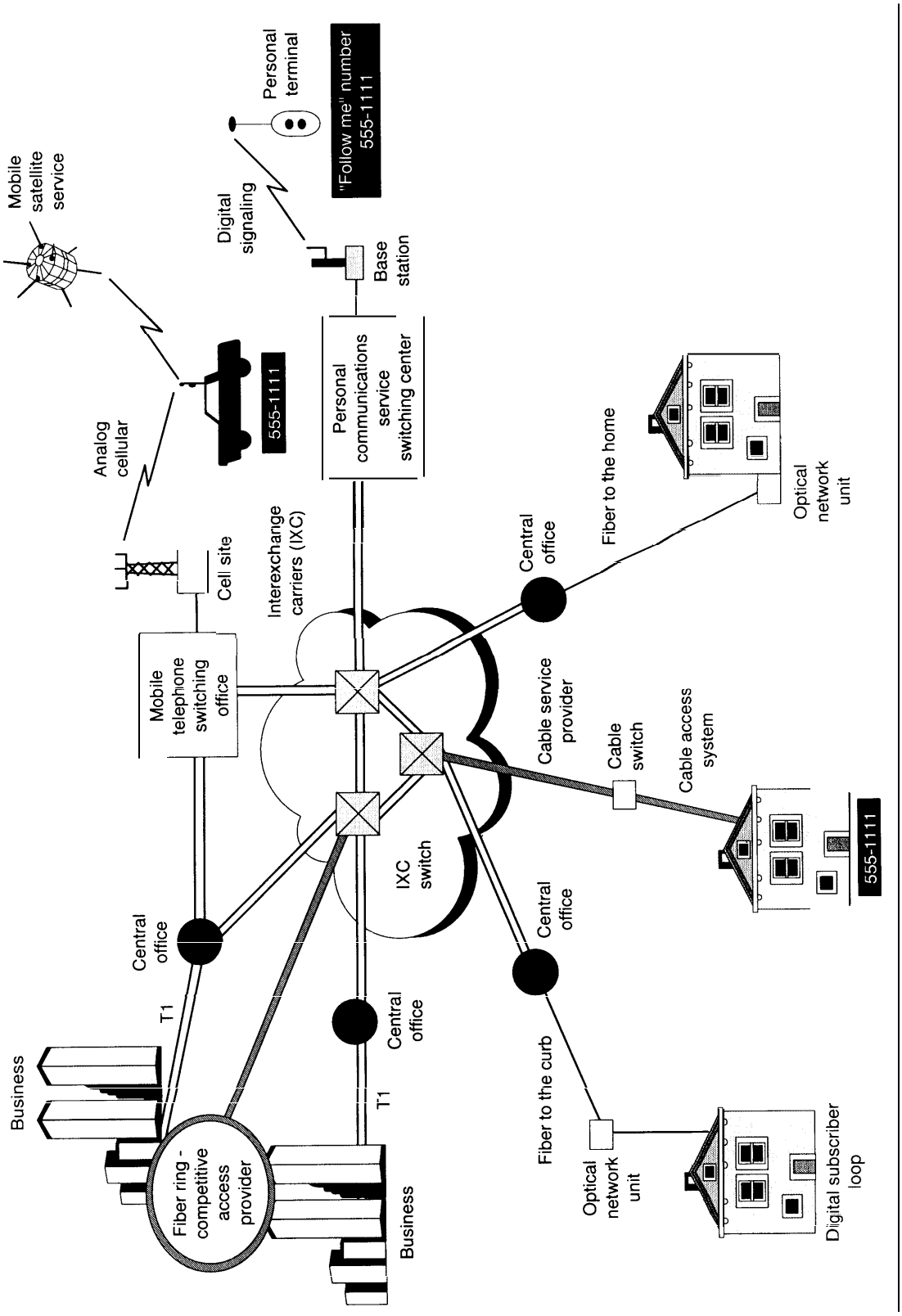
SOURCE Federal Bureau of Investigation, 1994

limited by the imagination of the systems engineers and developers and the acceptance of the new applications in the marketplace. Faster transmission systems and computer networking will lead to advanced systems that can leverage the bandwidth into currently unforeseen applications. The vision of a National Information Infrastructure (NH), if realized, could unleash a diversity of new services based on computer mediated multimedia communication far different from the current communication paradigm. A diverse offering of features and services is currently available on the U.S. telephone network, and this list will grow as time passes. (See table 2-1.)

TECHNOLOGIES

Each of the technologies or features listed in table 2-1 requires a technical modification or solution to meet the requirements of the Act. Some solutions may be easily achieved through software programs or minor hardware modifications. Other

FIGURE 2-4: Future Operating Environment



SOURCE: Federal Bureau of Investigation, 1994.

modifications will require redesign or re-engineering, or perhaps significant development efforts to meet law enforcement's needs. Some of the technologies listed in table 2-1 are already deployed throughout the national system. Others are installed or offered by some service providers and not by others, and sometimes carriers may be using different (incompatible) standards to drive or manage the same generic technology. Still other technologies are just emerging into a commercial stage of development and have not yet been widely adopted or deployed by the industry.

One such developing technology is the Asynchronous Transfer Mode (ATM) of transmission, which is considered by many in the telephone and computer networking industry to be the chosen technology for building the backbone of the next generation of telecommunication networks. This technology would radically change the characteristics and operation of the network by integrating voice, video, and data into the operating system. It offers phenomenal speeds (rate of information transfer), potentially up to billions of bits per-second range (gigabits). ATM is able to carry traffic originating from many different kinds of networks that will make up the National Information Infrastructure of the future.

Other digital network technologies are based on the transmission of information *packets* (frames or cells) that route segments of the information string (a voice message, an image, or data) to individual addresses within the interconnected network in a so-called "connectionless" mode. This is the transmission mode used on the Internet. Packets for an intended recipient may take a number of different routes to reach a destination, depending on the traffic congestion on the network and other network management factors.

Each new technological development presents the industry and law enforcement with a challenge to maintain parity for electronic surveillance in a fast-changing communication environment. The combined efforts and collaboration of the industry and the law enforcement agencies will likely be required on a continual basis for the foreseeable future as the nation's communication infrastructure undergoes a nearly complete metamorphosis.

The industry/government joint activities within the Electronic Communication Service Providers (ECSP) committee discussed in chapter 1 is addressing the practical matter of adapting the telecommunication industry's installed equipment base to comply with the Act. This, in its self, is a substantial and expensive task, but the technological challenges presented by the emerging network technologies, and technologies still in a conceptual stage, will be waiting to be solved when the immediate task is finished.

The ECSP committee has divided the technologies of immediate concern, i.e., switch-based solutions, advanced intelligent networks (AIN), mobile cellular communications, and personal communication services (PCS). The action teams are supplemented by others that deal with the interfaces between the carriers equipment and the law enforcement agencies, and one that considers the implications of future technological developments.

SWITCH-BASE SOLUTIONS

The function of a switching system is to interconnect circuits. It is the preferred point of access for electronic surveillance by the law enforcement agencies. A *switch-based* solution is an approach to meet law enforcement's electronic surveillance requirements using the traditional central office switch as the point in the network where access to the intercept target's communication is achieved.

There is estimated to be more than 20,000 landline switches installed and operating in the United

TABLE 2-1: Description of Currently Available Features and Technologies on the U.S. Telephone

Feature/technology	Description	Feature/technology	Description
Call Forwarding	Ability to redirect a Directory Number (DN) from one destination to another Directory Number.	Digital Loop Carrier (DLC) and Fiber-in-the Loop	These systems connect subscribers to the serving end offices. These technologies affeet traditional techniques for intercepting communications on the local loop.
Serial Call Forwarding	Ability to redirect a call multiple times.	private Virtual Network	A set of software-defined functions that give a subscriber control of a portion of the bandwidth and switching fabric of a service provider that allows the subscriber to manage that segment of the network as if it were its own.
Speed Dialing	Ability to establish and dial pre-selected numbers with an abbreviated code.	Voice Mail (E-Mail)	Voice mail services provided by a carrier using a peripheral component to switch or an Advanced Intelligent Network (AIN) platform.
Three-Way Calling/ Call Transfer	Ability to add a third party to an on-going call. The party initiating the service can drop off, thereby transferring the call.	Electronic Mail (E-Mail)	Public E-Mail services offered by common carriers.
Calling Line Identification	Ability to include calling line identification in call set-up information.	Facsimile Mail	Ability to send a FAX to a mailbox (storage location) with an associated Directory Number (DN). A recipient can access and retrieve the FAX at a later time.
Voice-Activated Calling	Ability to use voice commands to dial pre-selected numbers. (Under development).	Switched Multi-Megabit Services (SMDS)	SMDS is a high bit-rate (fast) connectionless, cell-relay digital transport service used for date, voice, and images.
ISDN-BRI Access Loop	Basic rate Integrated Services Digital Network.	High Bit-Rate Digital Subscriber Lines (HDSL)	A technology that builds on the ISDN basic rate that are designed for transport service used for date, voice, and images.

ISDN-PRI	Primary rate Integrated Services Digital Network.	Asymmetrical Digital Subscriber Lines (ADSL)	An application of ISDN that provides 1,544 Mbs line speed toward the user and only 64kbs toward the network, hence the reference to "Asymmetrical. " The standards was primarily aimed at the delivery of video to the home (e.g., Video Dial Tone).
CLASS Features	Automatic Recall, Selective Call Forwarding, Caller ID, Call Blocking, etc.	Intelligent Networks and Advanced Intelligent Networks (AIN)	Advanced networks based on common channel signaling using the international Signaling System 7 (SS7) standard that provides out-of-band, packet-switched communication among network elements. This allows central offices to query databases in the Service Management System (SMS) about the called or calling number and subscriber profile information.
Advanced Intelligent Networks (AIN)	AIN is a platform that supports advanced call features and applications.	Intelligent Customer Premises Equipment (CPE).	Intelligent functions (computer-based built into modern CPE may interact with non-standard switches, i.e., proprietary electronic terminals, etc., that make interception of signaling information more difficult.
Cellular	Ability to provide telecommunications services to mobile subscribers using cellular systems. Features include intra-system roaming, inter-system roaming, seamless roaming, and Cellular Digital Packet Data.	Universal personal Telecommunication Service (UPT)	A service that allows a user to access services from any terminal wherever he or she might be on the basis of a personal identifier. Those services that the user is qualified for would be available from wherever the person might be, The user's service profile could therefore be altered from remote locations by the user.
Personal Communications Services (PCS)	Allow access of services from different locations, while in motion, potentially on a global basis, through satellite communication.		

SOURCE Electronic Communications Service Provider Committee (ECSP).

States today.[8] Approximately 1,200 of these switches are of a special kind that support Integrated Services Digital Networks (ISDN), a channelized communication mode that serves the needs of some business customers and a fewer number of residential subscribers with special needs. ISDN separates the signaling information from the call content information, which increases the speed and flexibility of communication. It also increases the complexity of wiretapping. Integrated Services Digital network switches are being considered as part of the Switch-Based Solutions Action Team.

Switch Technology

The 20,000 switches in service today are a mixture of old and new technology. A few rural areas still have vintage 1900 step-by-step (SXS) electromechanical switches in their networks, although they are being quickly phased out. Some electromechanical crossbar switches from the late 1930s still exist on the network. The electromechanical switches remaining pose no problem to law enforcement because their technology is simple, they are largely located in rural areas, they do not provide flexible calling features, and they are being replaced by modern switches rapidly.

Modern electronic central office switches are able to provide a vast number of switch features and services. Electronic switches are based on either analog or digital technology. Analog Stored Program Control Switches (Analog-SPCS) were introduced in the mid-1960s, and became the mainstay for metropolitan switches in the 1970s and '80s. A large number of Analog-SPCS remain in service, but they are being replaced by digital electronic switches. Digital-SPCS were introduced in the early 1980s. There is a large number of Digital-SPCS in the national network, and their number is growing. These electronic switches are largely manufactured by four manufacturers: AT&T, Ericsson, Northern Telecom, Inc., Siemens Stromberg-Carlson.

A number of other type switches provide functions and services in addition to the circuit switches listed above. These include Packet Switches, Private Branch Exchanges (PBXs), Broadband Switches, Cellular Switches, and Personal Communication Services (PCS) switches. Among the ECSP Action Teams, Cellular and Personal Communication Services are being dealt with separately from Switch-Based Solutions in the central office. On balance, Packet Switches, PBXs, and Broadband Switches, while they will be more important in the future, do not figure as prominently in the network at this time, thus they present a lesser immediate practical problem for law enforcement, and are not directly addressed in the Act.

There are two major categories of switches: local and tandem. A local switch connects one customer's line to another customer's line, or to a connection (trunk) to another switching system. A tandem switch connects trunks to trunks. A third category of switch—remote switches—are local switches where a portion of the switch and some switch software is located away from the main or *host* switch. Host switches can serve several remote switches, and are connected to the remote switches with connection links. Electronic surveillance at the central office switch will involve local and tandem switches, as well as host and remote switches.

The major impact that new switching technologies have had on the network is the emergence of remote digital terminals and switch modules that terminate the conventional analog interface nearer the customer and use a digital interface to other network components.

[8] Testimony of Hazel E. Edwards, Director, Information Resources Management/General Government Issues, Accounting and Information Management Division, U.S. General Accounting Office, before a joint hearing of Subcommittee on Technology and the Law, U.S. Senate, and the Subcommittee on Civil and Constitutional Rights, Committee on the Judiciary, U.S. House of Representatives, Aug. 11, 1994, p. 5.

Features and Functions

Introduction of Analog-SPCS into the national telephone network nearly 30 years ago brought many new features and functions to customers. These features (Custom Calling Services) included Call Forwarding, Speed Calling, Call Waiting, etc. Since that time, hundreds of more sophisticated specialized services have been developed as Digital-SPCS came on line. Many of these have presented substantial challenges to law enforcement agencies' ability to conduct court-ordered electronic surveillance.

The features or functions described below present the most significant challenges to meeting the needs of the law enforcement community:

Call Forwarding

Allows a subscriber to redirect the incoming calls by dialing the call forward activation code followed by the directory number to which the calls are to be forwarded. This feature can be activated and deactivated at any time from the subscriber's telephone set.

Electronic switching systems have the ability to redirect an incoming call to either another directory number within the same exchange, or to another exchange over a trunk line. When a call is redirected by the switch, the call content is not transmitted to the subscriber's line, but instead is rerouted at the switch.

Speed Calling

Permits the subscriber to link a set of abbreviated directory numbers (i.e., one number or two-number sets on the telephone) to the directory numbers (DN) of frequently called parties at the subscriber's own initiative. This allows the subscriber to initiate a call by dialing the abbreviated one or two-digit number. Activation of Speed Calling is at the central office switch without involvement of the service provider. Some versions of speed dialing services permit the subscriber to change the assignment of directory numbers in real time, i.e., in the course of a call, or to change the number assignment remotely. Abbreviated Speed Calling codes created by the subscriber are accessible to law enforcement agencies from the local exchange carrier.

Three-Way Calling and Call Transfer

Enables a subscriber to add additional parties to a call that is in progress. When Three-Way Calling is invoked, the calling party or the called party temporarily suspends the conversation, initiates service and connects to another party, then adds the new party to the initial call. Call Transfer behaves somewhat as Three-Way Calling, but it allows the initiator of the transfer to drop off the call while the remaining parties continue the conversation.

Custom Local Area Signaling Service (CLASS)

Is a set of call management features that provides the called party with control over incoming calls. CLASS features are available through both Analog-SPCS, and Digital-SPCS that are equipped to support the Common Channel Signaling/Signaling System-7 (CCS/SS7) capabilities. CLASS features place more of the control of the call in the hands of the called and calling parties. Those features, which provide the called party more control, generally are enabled by passing the calling party's number to the terminating switch as part of the SS7 call setup message. About a dozen features are available through CLASS services.

Automatic Recall allows the user to activate a procedure by dialing a code, e.g., **69*, that automatically redials the last incoming call—whether or not the call was answered—without having to know the caller's number.

Selective Call Forwarding enables a customer to define a list of telephone numbers and assign each a *forward-to* destination number. Incoming number on the list are forwarded to the assigned destination number. Selective Call Forwarding, and some of the other CLASS features, provide the customer with the ability to create, modify, activate, and deactivate screening lists at will without the involvement or knowledge of the service provider.

Number Portability

Number portability will allow telecommunications users to retain their telephone numbers over time, despite moving to different service areas and physical addresses. Potentially, users could be assigned a lifetime phone number. The telecommunications industry is also developing services that use a nongeographic number to identify a subscriber, such as AT&T's Follow Me service. Callers can be reached at the number regardless of their physical location or the type of terminal equipment used (i.e., home telephone, office telephone, cellular terminal). The infrastructure to support these types of services will be deployed over the next several years.

The availability and use of portable and nongeographic numbers may have several implications for law enforcement. Law enforcement will have to be able to determine the carrier serving the investigation target, that person's location, and any subsequent carriers and locations involved in transmitting the communication. Network-based capabilities to support lawfully authorized interceptions should be capable of providing dialed number information as well as translated numbers used by the network for routing calls to or from the intercept subject.

Integrated Services Digital Network (ISDN)

ISDN provides a broad range of voice, data, and image services based on digital communication for transport and control within the network. ISDN is based on combinations of 64 kbs (thousand bits per second) channels (lines) combined to increase bandwidth, and therefore increase the speed and capacity of transmission. Information is converted into digital form within the subscriber's equipment before being ported to the network. Since everything is in digital form, all voice and nonvoice information looks the same as it passes through the system.

ISDN uses a separate 16 kbs digital channel (D-channel) for signaling, i.e., communication between the subscriber and the local switch. The D-channel is part of the access line, but it can be used to carry user-to-user information (e.g., packet messages) as well as signaling information. The subscriber controls the service features by sending messages to the switch, and the switch responds with messages to the subscriber over the D-channel.

The functions and signaling for ISDN are processed through a number of standard interfaces that provide different data rates (i.e., speed and capacity). The two most common, and of most concern to the law enforcement agencies, are:

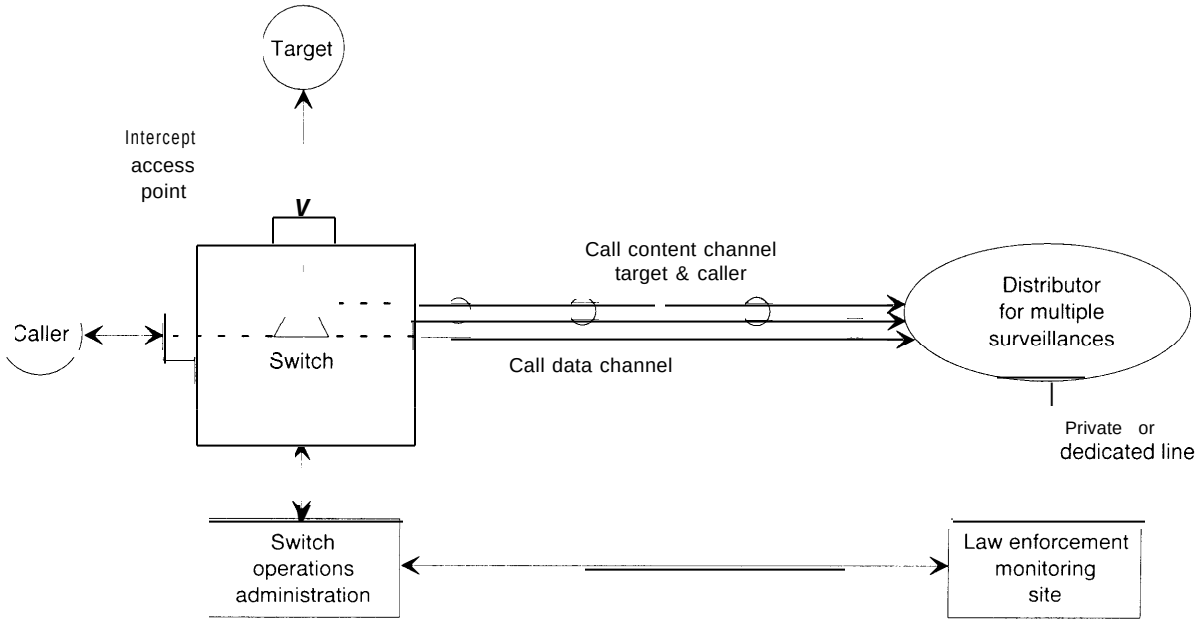
- Basic Access—composed of two 64 kbs B-channels (for voice, data, or images) and one 16 kbs D-channel for signaling; and
- Primary Rate—operates at a rate of 1.544 Mbs (million bits per second), composed of 23 B-channels of 64 kbs each, and one 16 kbs D-channel for signaling.

With ISDN the subscriber's signals for activating or deactivating a feature is carried over a separate channel (D-channel) instead of being carried over the same channel as the call content, as is the case for Analog-SPCS. Traditional analog intercept techniques are not compatible with ISDN.

Configuration of Switch-Based Solutions

P.L. 103-414 requires that intercepted call setup and call content information be instantaneously available to the law enforcement agency or agencies at one or more monitoring site off the premises of a service provider. Each simultaneous intercept originating from a switch must be carried individually and be adequately associated (identifiably linked) with each lawful intercept at an authorized law enforcement agencies monitoring point. An intercept target may be the subject of more than one authorized wiretap by more than one law enforcement agency. In such cases, both call content and call-setup information must be routed to both agencies without either knowing of the existence of the wiretap initiated by the other. This will require a distribution facility or some other means to route each intercepted call to each

FIGURE 2-5: Generalized Configuration and Functional Components for Electronic Intercepts at a Service Provider's Switch



SOURCE: Electronic Communication Service Providers Committee, 1995

agencies' monitoring site over a private line or connection. (See figure 2-5.)

An intercept is initiated by a service provider at the request of a law enforcement agency having legal authority for the wiretap. The service provider remains in administrative control of the intercept through an *interface,* i.e., a point or connection common between the service provider's system and the law enforcement agencies monitoring site. Communication links between law enforcement monitoring sites and the service provider will establish the surveillance parameters for routing information and access to the intercept target's speed-dialing lists and automatic call forwarding lists without direct control of the switch interface or the distributor component by law enforcement officials.

Call information, i.e., call content and call data, is routed automatically from the target line interface within the switch that connects the targeted line through the distributor component to law enforcement monitoring sites once a lawful wiretap is triggered by the service provider.

The switch and distribution functions in the intercept configuration shown in figure 2-1 is straight forward for Plain Old Telephone Service (POTS), but Integrated Service Digital Network (ISDN) at the basic or primary rates of service can carry 2 or 23 calls, respectively. Each channel is considered to be a separate call, therefores simultaneous processing and routing communications carried over ISDN, and also multifrequency PBX trunk lines will likely require more complex solutions.

WIRELESS TECHNOLOGIES

The mobility of an intercept target using mobile cellular communication presents problems for electronic surveillance that did not exist a decade ago. Its flexibility and adaptability for mobile communication, whether on foot, in a moving ve-

hicle, from a boat, or from an airplane, makes it an attractive alternative mode of telecommunication for the criminal element.

There are currently two primary modes of wireless, mobile communication available to subscribers: Cellular communications, currently one of the fastest growing sectors of the telecommunication market, and Personal Communication Services (PCS), a developing form of wireless communication with similarities to cellular, but with differences in operations that may present unique wiretap problems to law enforcement as special features are developed. A fourth communication system in the conceptual stage of development uses satellite-based technology for long-range communications over broad geographic areas. When operational, satellite systems will increase the complexity of electronic surveillance by the law enforcement agencies, since they will be capable of transnational and global communication (portending possible problems with international transfer of information or data). Furthermore, these systems may employ space-based switching and hand-off technology that places the control center for communications in remote reaches of orbital space instead of secure, controlled operation accessible directly on land.

Mobile Cellular Technologies

Wireless cellular service covers 306 metropolitan areas and 428 rural service areas. Two cellular service providers are licensed to offer service within each service area. One of the service providers is the local telephone company serving that area (e.g., Southwestern Bell for example), and the second is a non-wireline company (e.g., McCaw for example). These providers use multiple cell sites (*supra*) and one or more mobile switch carriers (MSCs), depending on customer demand. Reseller providers exist, i.e., those who lease and retail capacity and services from other providers, but they largely depend on the facilities of the primary service providers.

Cellular service allows a subscriber to move freely within a defined cellular service area centered around a cell site (each cell ranges between one and 20 miles in diameter). If the subscriber moves into an area serviced by a different cell site that is within the service provider's service area (Intrasystem Roaming),[9] the call control may be passed to a new MSC.[10] If the user activates the mobile unit out of his or her home area (Intersystem Roaming), information about the user (MIN, ESN, authorized services, billing, etc.) is exchanged between the original (home) service provider's Home Location Register (HLR) and the Visited Location Register (VLR).

The main elements of a cellular network include:

1. cell sites that provide the radio frequency link between the mobile user and the cellular network; and
2. Mobile Switching Center (MSC) that performs call switching and routing, and external connections to other networks (e.g., local exchange carriers and interexchange carriers). (See figure 2-6.)

Each cell antenna facility is connected either by wireline or microwave radio to the MSC.[11]

Cellular radio communication may be either analog or digital. The radio components of most of today's cellular networks are analog-based, but many of the carriers are slowly switching from analog systems to digital systems in order to increase the capacity, offer a wider choice of services, reduce fraud, and improve security.

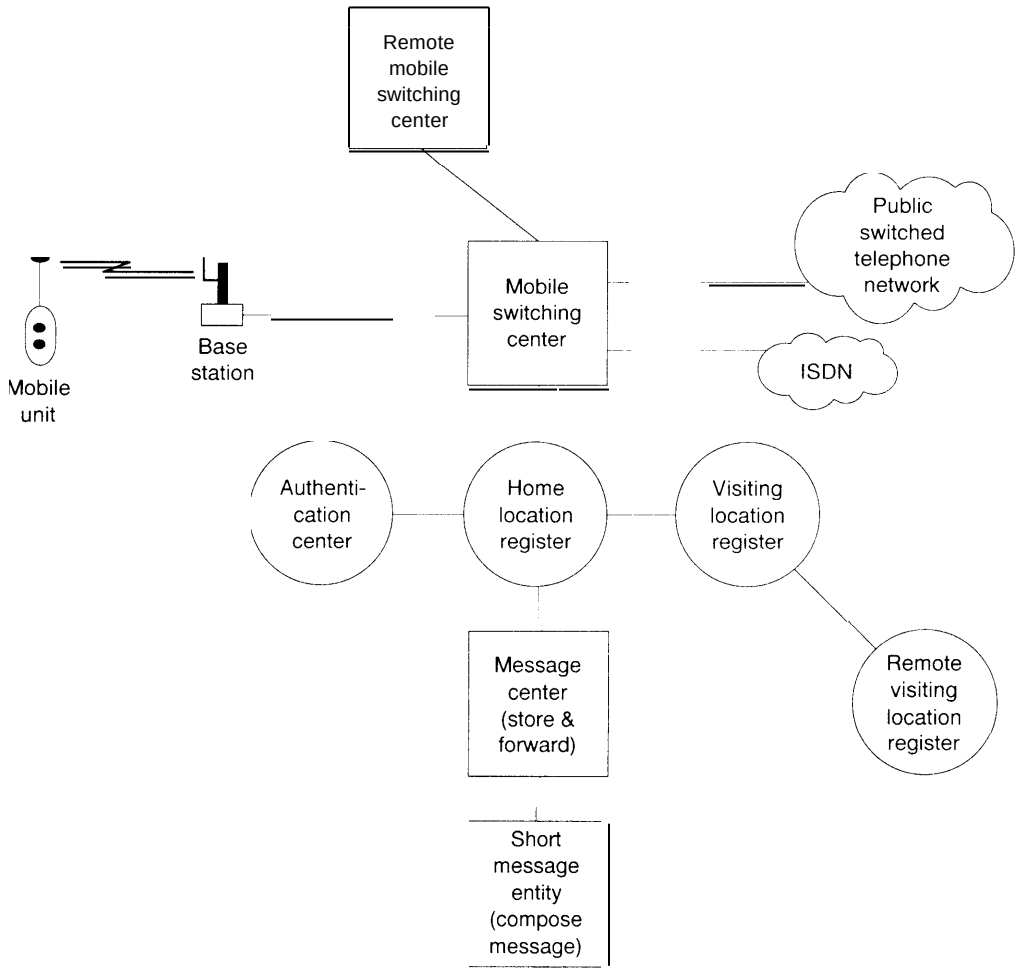
---

[9] The term "roaming" generally applies when the subscriber initiates or receives a call in other than his or her home area.

[10] Roaming within the service area of another service provider is contingent on the home cellular provider having entered a "roaming agreement" with the second carrier. Roaming privileges are not uniform and reciprocal among all providers.

[11] Some rural cellular companies' may not own a MSC switch, but instead may lease the use of an adjacent cellular companies switch. In this case the leasor service provider would have control of the switch, and any intercepting activities would have to be performed by the leasor although an authorized wiretap may be served on the leasee. This problem may need to be addressed by promulgating regulations.

FIGURE 2-6: Typical Architecture for a Cellular Service Area



SOURCE Electronic Communication Service Providers Committee, 1995

Frequency Modulated (FM) radio channels are currently used for voice communication and control (call supervision and handoff) [12] from the subscriber telephone to and from the receiving radio at the cell site of the service provider. Control channels relay control information between the MSC and the mobile unit. Control channels are used during call setup to transmit dialed digits and the mobile unit's Mobile Identification Number (MIN) and Electronic Serial Number (ESN).

The analog signal received at the cell site is converted to digital form and transported to MSC over multiplexed channels of T1 or T3 land lines or digital microwave radio systems. The multiplexed signals contain voice or data communication, and information about the user (e.g., MIN

[12] "Handoff' occurs when a subscriber travels from one service area to another while a wireless call is in progress.

and ESN) and the dialed digits (Directory Number) needed to complete the call.

Once a call has reached a MSC, the connection to its destination is handled as any call placed on a land line through a local exchange carrier end office. Based on the number called, the MSC connects the caller through:

- a wireline local exchange carrier switch;
- an interexchange (long distance) carrier point of presence (a connection point between long distance carriers and the local exchange);
- a MSC outside the service provider's service area; or
- another mobile subscriber within the same MSC.

A call may pass through several switches and facilities of many service providers before reaching its destination.

Although cellular networks are similar to the line-based local exchanges in some ways, they function differently in others. In a cellular system, subscribers control access and selection of services (e.g., activating, answering, addressing) by sending and receiving control messages from the mobile unit over the control channel to the MSC. The MSC receives and decodes the information from the control channel, identifies the user (from the MIN transmitted by the mobile unit), and activates the services, features, and restrictions associated with the subscriber's MIN. After the preliminary setup information is processed by the MSC, a connection to the Public Switched Telephone Network (PSTN) is established and the dialed digit information (Directory Number, etc.) is relayed to the next switch or connect point in the PSTN. The MSC then monitors the control channel from the mobile unit and awaits further control signals that indicate a request for disconnect, movement to another cell, or activation of a feature, e.g., three-way calling.

Configuration of Cellular Solutions

P.L. 103-414 does not address technologies for intercepting the radio transmission associated with the operation of a cellular system. The preferred point of access for a lawful interception by the law enforcement agencies is at the MSC. The requirements of the law enforcement agencies under the Act focus on switch-based technology at the MSC and relational databases that interact with the MSC.

Some cellular switch manufacturers have developed capabilities within their switches to accommodate some of the needs of the law enforcement community for lawful intercepts. The requirement under P.L. 103-414 to support multiple, simultaneous intercepts may, however, overtax the intercept capabilities now built into MSC switches.[13] The capacity to accommodate multiple intercepts is determined by the number of electronic intercept access ports designed in the MSC switch. Switch manufacturers are working on modifications to overcome port limitations, but in some cases physical limits of space within the switch will limit the number of access ports that can be added. Switch design was based on the anticipated increase in capacity needed for subscriber growth. Law enforcement agencies' need for increased capacity for electronic surveillance was not hitherto considered in switch specifications.

Call Setup Information

As is the case with landline telecommunications, law enforcement agencies require access to line information for all completed and attempted calls, including calls forwarded to another number or voice mail, unanswered calls, and call waiting calls. Such information includes: The cellular intercept subject's Mobile Identification Number (MIN) and Electronic Serial Number (ESN), and

[13] Maintenance ports built into the current generation of cellular switches allow access to information needed by law enforcement agencies. However, the number of access ports are limited, and information at these ports can only be recovered by manual queries. This limits their usefulness for dealing with handoffs from MSC to MSC, slows the recovery of information, and requires the involvement of several law enforcement officials to implement some cellular intercepts.

the calling party's line information *when delivered* to the MSC that is being tapped.

Call setup information for calls originated by a cellular intercept target must include all digits dialed by the subject (e.g., Directory Numbers, speed dialing, etc.), billing record information, and signaling information used to establish or redirect call flow (e.g., activating service features). During the course of originating a call, signaling information is carried over the control channel to the MSC.[14] After connection is made with the called party (cut-through), subsequent dialing information from the target's mobile unit (e.g., pulses/tones representing digits, voice dialing, etc.), including information generated by the subject in response to system queries, travel over the bearer channel (call content channel). The call management information transmitted on the bearer channel is not interpreted by the switch, and therefore is not available to the law enforcement agency in the call setup messages. This information is in the form of audible tones or voice information commingled with call content.

Call Content

Law enforcement agencies require access to cellular call content of the intercept target's terminal, including voice, voice band data, and paging/short messages.[15] Access to call content must be provided by the cellular service provider for calls originated or terminated to the intercept target's mobile number, including mobile-to-mobile calls, mobile-to-wireline calls, and wireline-to-mobile calls. All of the custom calling functions invoked by the subject, e.g., call forwarding, voice mail, three-way calling, call waiting, etc., must be accessible while the service provider maintains access to the call.

For redirected calls, access is required from the time that the bearer (call content) channel to the target (either the primary called number or to a redirected number) is established, until the call to the forwarded-to target is released. If access to the communication cannot be maintained, the cellular service provider is required to provide the law enforcement agency with information that will enable law enforcement to determine the new service provider's area, whether landline or cellular. Law enforcement agencies would prefer to have access maintained by the cellular service provider for three-way call for the duration of the call whether or not the intercept subject's call is dropped. Industry technicians are not sure that this is feasible in a cellular system.

Mobility

Cellular service providers are to provide continuous access to all ongoing calls, so long as the carrier maintains access to the call, regardless of the number of handoffs that may occur, whether intra-cell, intra-MSC, or inter-MSC. Inter-MSC handoffs include: handoffs *within* a service provider's area when more than one MSC serves an area; handoffs between *different* service areas operated by the same service provider; and handoffs between *different* service areas operated by *different* service providers. The intercept must be maintained regardless of how many intervening handoffs might occur. After handoff, law enforcement agencies require access to information identifying the visited service area and the new service provider's identification so that a lawful authorization (*secondary carrier assistance order*, which is derived from the original court authority) for intercept information in the new service area under the control of the second or successive carriers can be obtained.

---

[14] Each cellular service provider within a market area is assigned 416 channels for communication. Twenty-one of the channels are control channels that continuously connect each activated handset with the cellular system.

[15] Short Message Service is a function offered by some cellular service provider. It is similar to paging, with abbreviated messages being transmitted over the control channels.

Roaming

When roaming outside of the home service area, law enforcement requires access to all calls initiated or received by the subject if the visited service provider has received a lawful request to activate an intercept, and arrangements have been made for delivery of the information to the law enforcement monitoring site. The visited service provider has no legal obligation to intercept a cellular target's calls once the subject moves out of its service area unless it is a call in process (*supra*). The home cellular service provider is required to provide access to any call setup information or call content if access is maintained in the home area during call delivery to a roaming subject.

Registration Information

When a mobile intercept subject roams into a new service area, activates his or her mobile unit, and requests service, the home service providers Home Location Register (HLR) exchanges information with the new cellular service provider's Visiting location Register (VLR). When this occurs, law enforcement agencies require information on the identity of the new service area requesting the registration information. Law enforcement must then obtain a lawful authorization to access the call content and call setup information from the visited service provider.

Service Site Information

Law enforcement agencies in possession of the proper Title III court authorized electronic surveillance order (P.L. 90-351, Sec. 801 et. seq.) or an *enhanced pen register*[16] (but not under law enforcement's pen register or trap and trace authority) may ask a service provider for detailed service site information regarding an intercept target's location. For example, a carrier provider may be required to deliver information identifying the cell site from or to which service is being provided, the cell sector, or analog radio frequency power levels coming from the intercept subjects terminal (a measure of distance from the receiving cell's antenna), the identity of the service area supporting communications after a handoff, and other geographic information available, including the subject's physical location if known.

Cellular Intercept Functions

The functions for intercepting electronic communications in the cellular environment parallels that used for landline switches (*supra*), but may require different architectures. However, setting up a call and managing it in the course of cellular communications will involve several steps, some of which are not used in landline switches, e.g., activation, registration/deregistration, and call handoff.

A service provider that controls a subject's HLR must identify and somehow set a flag within the subject's service profile to indicate that intercept processing is required at the MSC. If the intercept subject is visiting another service area of a cellular carrier that has been lawfully requested to initiate an intercept, the visited service provider may tag the subject (a temporary tag) within the VRL to indicate that information processing is needed when the subject activates services within its area.[17]

The lawful intercept request to the cellular service provider will typically call for:

- Intercept Subject Identifier (MIN),
- requesting law enforcement agency's name or numerical identifier,
- the law enforcement agency's monitoring location (line or identifier), and
- authorization and access information (e.g., service provider's personnel authorized to access or change intercept data).

---

[16] The basic authority for instituting a pen register surveillance is contained in 18 USC 3123. More latitude is granted for pen registers to obtain more detailed information on a subject is authorized under the procedures set forth in 18 USC 2703.

[17] This process is still under consideration by industry and law enforcement agencies.

Law Enforcement Access

Call setup information, signaling data, handoff information, call forwarding, call waiting, call content information, etc., will be transmitted in real time, or as soon as possible, to the law enforcement monitoring site. Call setup information (i.e., MIN, ESN, called or calling number, date, time, and available location information) may be transmitted over the signaling channel of law enforcement's monitoring line.

Personal Communications Service (PCS)

The Federal Communications Commission (FCC) is currently in the process of auctioning a 160 Megahertz portion in the 2 Gigahertz band of spectrum for the development of a new wireless PCS subscriber service that will perform similarly to cellular systems and will likely become the next generation of competitors to cellular services. Service providers have developed conceptual plans and in some cases have demonstrated PCS systems. However, development and implementation of such plans are at least two to five years away from commercial service. PCS, therefore, is at an immature stage of development that will allow the features needed for electronic surveillance to be built as an integral part of new systems.

PCS systems will operate at much higher radio frequencies (2 Gigahertz) than cellular systems (800 Megahertz). The higher operating frequency reduces the distance that a subscriber can be from a base radio station (cell) and maintain communication. PCS systems, therefore, will consist of many more smaller cells (microcells that cover a diameter of up to one mile around the antenna) to cover an area than is now commonly used by cellular service providers to serve the same size area. Unlike current cellular systems, PCS systems will be fully digital, and PCS handsets, will operate at lower power levels.

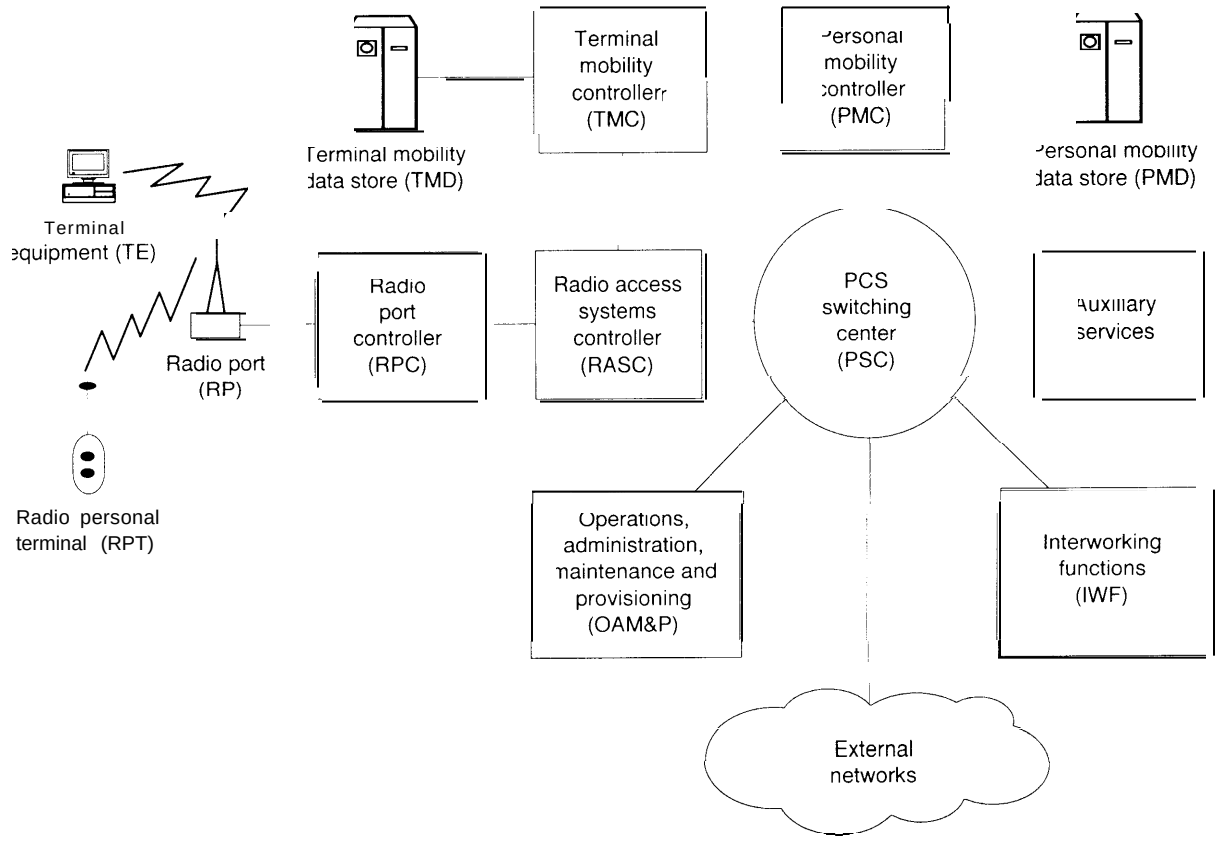
The major difference between the features offered by cellular services and PCS is the one-number service to be offered by PCS. A single-number system allows maximum personal mobility. Under this concept, a single directory number would be used to direct all calls to a user wherever he or she is. Cellular systems currently offer a measure of personal mobility by forwarding calls to a user's cellular telephone when they travel. But this feature operates independently of the Public Switched Telephone Network (PSTN) landline system and is only accessible through cellular service providers with databases that track a subscriber's location. Landline switching routines were based on having a directory number associated with a fixed location, not a mobile terminal.

The concept of one-number service (it has also been dubbed *Follow Me*) would integrate the landline network into the switching fabric of PCS by establishing a *nongeographic* prefix—*500*—in place of the area code. The 500 number would indicate to the landline carrier that the call needs special handling to route it to a PCS or cellular carrier.[18] To do this, the landline carrier's *Intelligent Network* technology (*infra*) must be integrated with the PCS and cellular system, all using common routing databases. Should this level of integration be obtained, a personal handset or a cellular terminal could be used either as a mobile instrument, or a substitute for the cordless residential telephone.

PCS is in an early stage of development. There is considerable uncertainty as to what the standards will be for the industry. Given PCS technology's stage of development, accommodating the law enforcement agencies' needs for electronic intercepts can follow a more logical development and progression than is possible for either cellular or landline networks that have an installed techno-

[18] Landline carriers now use a "500" dialing sequence to allow subscribers to use a touch-tone phone to update a database that indicates where incoming calls should be routed for cellular service. These functions are not integrated into the landline service provider's switching system, however.

FIGURE 2-7: Possible Architecture of a Personal Communication Service Network



SOURCE Electronic Communications Service Providers Committee, 1995

logical base that must be adapted or modified to comply with the requirements of the Act.

Configuration of a PCS System

The main components of a PCS network are similar to those of a cellular network, although different names are assigned to analogous parts of the system that perform the same function in each. The PCS Switching Center (PSC) operates very much like the Mobile Switching Center (MSC) in the cellular system. Both serve as a gateway to connectivity with the Public Switched Telephone Network (PSTN) and other external networks. (See figure 2-7.)

The Terminal Equipment (TE), i.e., user equipment, such as a computer or data terminal, can communicate with the PCS infrastructure in either a wireless of wireline mode. The Radio Personal Terminal (RPT), (a lightweight, pocket-size portable radio terminal) directly accesses the Radio Port (RP) for connecting the user to telecommunications services while stationary or in motion. The TE may use either Integrated Services Digital Network (ISDN) or non-ISDN transmission protocols. Wireless access is through Radio Terminations (RT), which terminates voice and data for the TE and forwards the signal information in digital form to downstream components, i.e., the **PCS**

Switching Center (PSC) for processing. Wireline access from a TE is linked directly to the PSC.

The Radio Port Controller (RPC) coordinates the wireless traffic received from the Radio Ports. It may also control handoff of mobile-to-mobile, or mobile-to-fixed-location calls placed among or between users through Radio Ports under its control. The RPC coordinates all calls placed or received by wireless users, and serves as the gateway to the PCS Switching Center.

The Radio Access System Controller (RASC) coordinates the functions among the Radio Port Controllers under its control. It supports the exchange of call, service, and handover control signaling and the transfer of terminal and user information. The RASC may also perform the internal bookkeeping function of charge recording, as well as linking with Terminal Mobility Controllers (TMCs), and the Personal Mobility Controllers (PMCs), which manage the terminal registration, authentication, locating and user/terminal alert functions stored in the Terminal Mobility Data Store (TMD) and Personal Mobility Data Store (PMD), respectively.

The PCS Switching Center (PSC) performs the connection control switching functions for accessing and interconnecting outside network systems to provide end-to-end services. Since PCS systems are designed to provide services to users based on the user's personal identity, rather than on a physical location as does wireline services (and to some extent cellular services), the PSC must interact with the PMC (and its supporting PMD) to access the user's service profile for registration, authentication, call alerts (ringing), and call management. The PCS must also have access to the service limitations and restrictions for a specific user, so therefore it may also have to interact with the TMC for information about wireless terminals.

A PSC serves five functions:

1. basic call and connection control for access and interswitch routing,
2. service control for personal communications users and terminals,
3. switch bearer connections to support handoff among Radio Port Controllers,
4. mobility management associated with personal communications users and terminals, and
5. network control and associated interworking for access to external networks.

The Terminal Mobility Controller (TMC) and an associated database (Terminal Mobility Data-Store, TMD), and the Personal Mobility Controller (PMC) and an associated Personal Mobility Data-Store (PMD), provides control logic to the system elements. The TMC/TMD handles authentication, location management, alerting, and routing to the appropriate RPT/RTs. The PMC/PMD provides information for personal user authentication, service request validation, location management, alerting, user access to service profile, privacy, access registration, and call management (routing to destination).

Internal systems functions, e.g., systems monitoring, testing, administering, and managing traffic and billing information, is handled through Operations, Administration, Maintenance, and Provisioning (OAM&P) components. Internetworking Functions (IWF) serve to ensure that all networking technologies work consistently and seamlessly to provide PCS users reliable service.

The PCS system, like the cellular systems, will be able to connect with a variety of outside networks that offer a range of services, including wireline (local and interexchange carriers), cellular, Competitive Access Providers (CAPs), etc.

It is yet uncertain whether PCS will provide Auxiliary Services. These include voice mail, paging, short-message service, etc.

Configuration of PCS Intercept Approaches

If all calls to and from a PCS intercept target are processed by the PCS Switch Center (PSC), with no calls to or from the target being switched at the Radio Port Controller (RPC) without first routing through the PSC, then electronic surveillance for PCS systems is analogous to the switch-based

solutions being considered for cellular and wireline services.

Registration and Activation—The Personal Mobility Data Store (PMD) and the Personal Mobility Controller (PMC), which store and control personal service information, can be used to flag an intercept subject for surveillance. If a home PCS service provider is requested by a law enforcement agency to implement an intercept, the intercept subject's PMD/PMCT entry would be modified to show:

- Intercept Subject Identifier (personal and/or terminal number);
- Requesting Law Enforcement Agency;
- Monitor Site Location (line/directory numbers); and
- Authorization and Access Information. This information would be sent to the home service provider's TMC/TMD and noted as a *temporary intercept request.*

Upon receiving a request for services from the intercept subject, the TMC/TMD would activate the intercept.

In the case that a nonhome PCS service provider that does not have control over an intercept subjects PMD/PMC is requested by a law enforcement agency to initiate an intercept, the service provider would enter the subject's personal service information and intercept information in the its TMC/TMD. The TMC/TMD would activate an intercept when a subject requests service (a PMC/PMD might also activate intercepts under certain conditions).

Intercept Access Functions—A PCS intercept is activated when the subject originates a call, receives a call, is provided handover treatment, is disconnected from a call, uses a vertical service (e.g., call forwarding, call waiting, three-way calling), registers, or changes his or her service profile information. The handling of vertical service features is similar to the manner in which those services would be handled through switch-based solutions and cellular service.

When an intercept is activated, connection is made to the authorized monitoring site for call content and control information. Call setup information would be sent to the monitoring site as it becomes available.

PCS Information Elements

PCS operations use about 70 different message types to maintain communications and services. At least 14 of these messages may be of use to law enforcement agencies. (See table 2-2.)

Location information, when authorized to be provided to law enforcement officials, is derived by correlating the Routing Number Bearer Channel and Channel ID to the PCS system component, e.g., Radio Port (RP), supporting the connection to the mobile subscriber.

Advanced Intelligent Network (AIN)

AIN architecture distributes the service logic throughout the network to support the many features and services available to subscribers. Therefore, it may be more difficult to identify calls that are associated with an intercept subject or to determine the origin or destination of calls to or from the subject. Additional functions will have to be built into switch-based solutions to meet the requirements of P.L. 103-414.

AIN is a system of interrelated computer-based components linked to a switched or wireless telecommunications network that provides a framework for services, e.g., call forwarding, credit card authentication, personal identification numbers, speed calling, voice dialing, etc., independent of the call process. AIN functions reside in network elements, which can communicate among themselves and with a controlling switch. In some cases, subscribers can access and control the databases for AIN services (e.g., speed calling lists) without the intervention of a service provider.

TABLE 2-2: PCS Information Elements of Possible Use to Law Enforcement

Information Element	Description
Radio Access System Controller Identification	Identifies a specific RASC.
Radio Port Controller Identification	Identifies a specific RPC.
Radio Port Identification	Identifies a specific Radio Port.
Channel Identification	Identifies a specific channel (a timeslot in the signal of a TDMA [Time Division Multiple Access] system, or one of several coded signals multiplexed into a CDMA [Code Division Multiple Access] system).
Radio Personal Terminal Identification	Identifies a specific radio personal terminal or mobile handset (either imbedded in the chipset in the handset, or may be programmed into a user's terminal).
Routing Number	A 10-digit geographical telephone number used by the Public Switched Telephone Network to route calls.
Bearer Channel Identification	A logical name used within the PSC to identify a connection end-point.
Radio Channel Identification	A logical name for the radio path. Timeslots and physical connections use this name to trace the information flow path from the radio transceiver to the interface mapping to the Bearer Channel.
Call Record Information and Charging Information	Contains the start and duration of a call. It might also contain information about the profile of type and frequency of services used by the subscriber.
Universal Personal Telephone Number	Telephone number associated with a user, not a terminal or a line as in wireline service.
Personal Identification Number	A confidential memorized number used by an individual to verify their identity to the system.
Authentication Key	Information from a magnetically encoded card (substitute for a Personal Identification Number).
Access Signaling Information	Used to pass supplementary service requests in the signaling channels rather than in the call content channels.
Signal Strength Measurement and Measurement Reference	Measure of the amplitude of the signal detected by the Radio Terminal or Radio Port. The reference refers to the decibel measurement used to measure signal strength.

AIN[19] architecture consists of signaling systems, switches, computer processors, databases, and transmission media, which provides customized software-controlled services. (See figure 2-8.)

Deployment of AIN is not uniform throughout the Public Switched Telephone Network (PSTN). It is being phased into the national system through progressive upgrades in software modules and intelligent network elements, which increase the functionality and flexibility of AIN.[20] Since AIN permits peripheral intelligent elements (software-controlled Intelligent Peripherals (IP)) to share control of a call with switch-software control, AIN might present special problems to intercepting the communications of wiretap target subjects.[21]

Signaling System Seven (SS7) switches and the national network based on the SS7 standard enable broad deployment of interactive AIN functions in the Public Switched Telephone Network (PSTN). The SS7 network signaling and processing is carried by an ISDN network. There are three major groups of technologies in the AIN architecture (See figure 2-8.):

1. Network Elements (NE), Service Switching Points (SSPs), non-SSP switches, and Signaling Transfer Points (STPs);
2. Network Systems (NS), Service Control Points (SCPs), Adjuncts and Intelligent Peripherals (IPS); and
3. Operations Systems (OSs), capabilities that provide network and service operations as their primary functions (Operations Systems may be unique to a service provider).

In general, AIN is not considered to be a part of the switching system. A switching system may include AIN capabilities, which generally consist of *triggers* in call processing and feature software, that if set, transfers functional control to another network platform. Many of the intelligent functions are part of the Stored Program Control Switches (SPCS), thus technical approaches for meeting law enforcement's intercept needs at SPCS are switch-based solutions (supra). However, some of the intelligent peripherals (IP) and adjunct components contain interactive software that allows subscribers to directly alter databases that control services and features available to them. It may therefore be necessary to query these peripheral components directly (or via a SPC) to provide law enforcement agencies the most current information available about an intercept target. This will require special access features that are not necessarily part of the switching process at the SPCS.

A Service Switching Point (SSP, See figure 2-8 above.), is a special kind of switch (e.g., an end office switch or a tandem switch) that contains AIN switch capabilities. A SSP can identify calls associated with AIN services. When a call is identified that requires AIN treatment, the SSP initiates a dialog with a Service Control Point (SCP) or peripheral where the information and software logic for the requested service is located. A *non-SSP switch* is one that does not have AIN capabili-

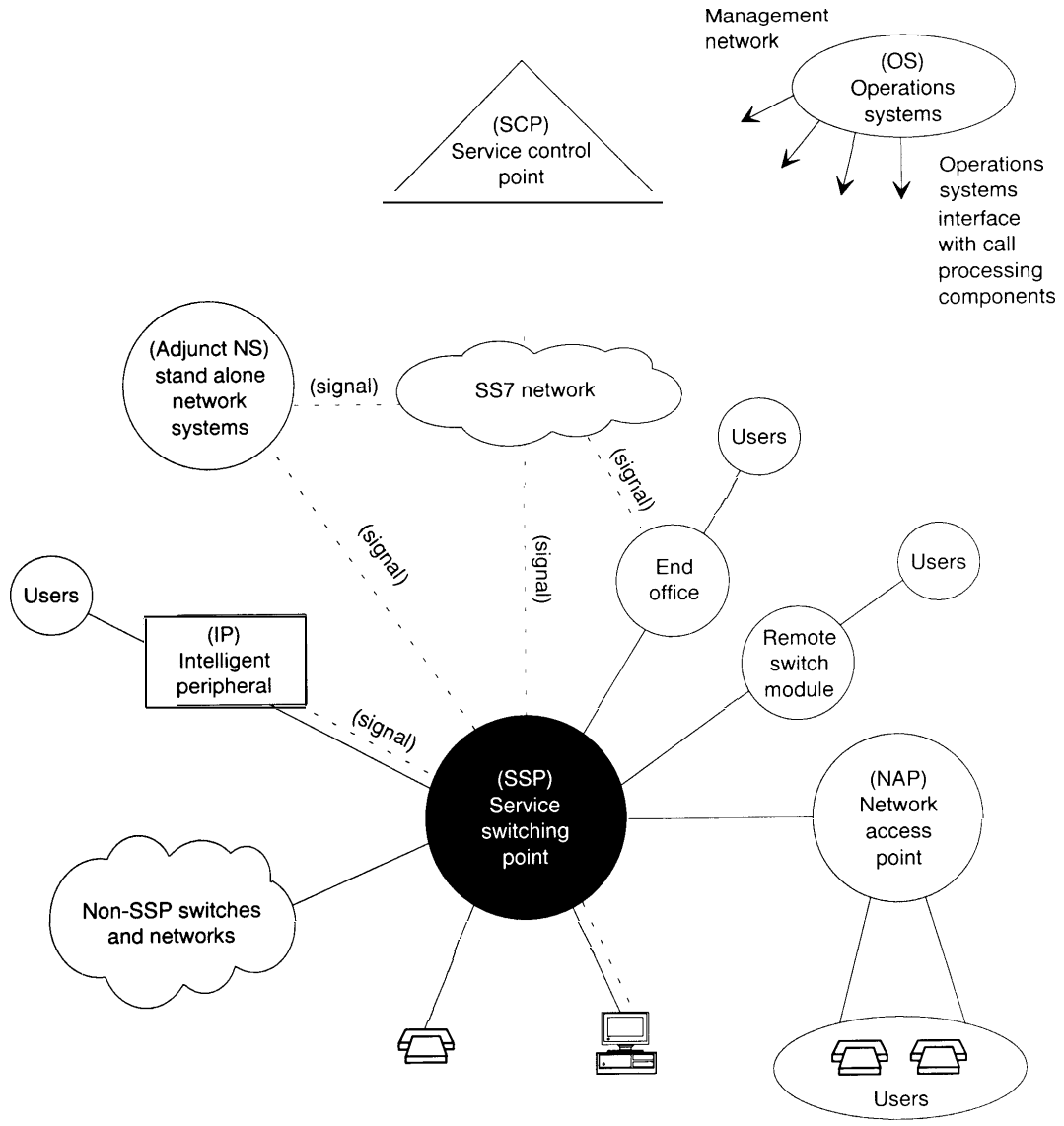
---

[19] AIN architecture has been primarily developed by Bellcore in collaboration with its clients, the Bell Regional Operating Companies (RBOCs). The interexchange carriers (AT&T, MCI, Sprint, etc.) have similar Intelligent Network (IN) systems in their networks. AIN can also be deployed in Cellular and Personal Communication Services (PCS).

[20] Beginning in 1983, intelligent elements have been progressively introduced into the Public Switched Telephone Network (PSTN). In the 1980s, Phase 1 of Bellcore's IN architecture (IN/1) was introduced. This was followed by AIN Release 0, AIN 0.1,. . .AIN 0.X. The introduction of AIN Release 0 in 1991 marked the transition from providing telephone service totally under switch-control software to providing services through shared control among intelligent network elements.

[21] For instance, Service Creation Environments (SCEs) allow nonprogrammer users to create a new service using icons representing functional service blocks without the intervention of the service provider. Service Management Systems (SMSs) allow users direct access to their services so they can make real-time adjustments as their requirements change.

FIGURE 2-8: Typical Advanced Intelligent Network (AIN) Architecture



SOURCE: Electronic Communication Service Providers Committee, 1995

ties, but is able to detect when a call requires AIN processing and route them to a SSP for processing.

Developing Technologies

The field of telecommunications is moving rapidly. A stream of new technologies is queued to complement or compete with the established communication systems of today. Some of these technologies have been waiting in the wings for their time to come as market demand and opportunities present themselves. Others are of newer vintage, such as some of the developing packet switching and satellite-based wireless commu-

nication systems. The new technologies may—or likely will—present new obstacles to law enforcement's needs for electronic surveillance in the future.

Since the deployment of these new technologies is still in the future, the range and magnitude of the problems that they may present to law enforcement is a matter of speculation. A couple of the more prominent technologies that are either in a preliminary stage of deployment or are poised for commercial deployment are briefly described below.

Satellite-Based Wireless Technologies

Satellite technology has been part of the communication system since the middle 1960s. Satellite communication is an integral part of the international telephone network.[22] Today, when high-speed optical fiber capable of carrying immense volumes of communication to Europe or the Far East fail, satellite communication links stand ready to carry the redirected traffic.

Most of the early satellite systems were matched to the commercial need of *wholesale* communications, i.e., from one service carrier's switch to another carrier's switch, hence to wirelines. New satellite systems on the drawing board or in early phases of implementation will link directly with the user. Some propose to operate much like cellular or PCS systems, linking the user and his or her handset directly to the space-based satellite system.

Two classes of satellite-based communication services are being considered: GEOS—Geosynchronous Earth Orbiting Satellites; and LEOS—Low Earth Orbiting Satellites.

Geosynchronous Earth Orbiting Satellites (GEOS)

GEOS systems will be placed in a geosynchronous orbit at the prescribed distance of 22,300 miles above the equator. These satellite systems will use a higher transmitting power level than will the LEOS (because of the difference in distance to the earth). GEOS can be deployed either in a *constellation* (several satellites), or as a single satellite, depending on the nature of the service that they will deliver.

Deployment of a constellation of GEOS in several different orbit locations can provide global communication. The system satellites would be linked by inter-satellite communications to manage the switching and administration. Interconnection with the Public Switched Telephone Network (PSTN) can be provided, and subscribers can manage their own communications through personal ground stations.

A single GEOS satellite can be equipped to aim *spot beams* to achieve regional communication coverage. Such systems operate much like a cellular system (each beam representing a space-deployed cell site), with switching systems analogous to the Mobile Cellular Switches (MCSs) of a ground based cellular system.

The technical impacts of these technologies on law enforcement agencies' ability to conduct authorized wiretaps will come from two sources:

1. Caller-to-caller direct links through a satellite switch that bypasses the terrestrial switched system; and
2. Jurisdictional problems of conducting authorized wiretaps across the boundaries of sovereign nations.

Low Earth Orbiting Satellites (LEOS)

LEOS are placed in lower orbital positions (500 to 1,400 kilometers [310 to 870 miles]) than are Geosynchronous Earth Orbital Satellites (GEOS). The lower orbital paths allow them to be operated with less power and reduce the time delays that plague communications (time delays limit the usefulness of GEOS communications for some time-sensitive applications) using GEOS, which orbit at distance up to 60 times greater than LEOS.

[22] Satellites are used extensively for video, data communication, and for communication with ships at sea. For the purpose of this discussion, the use of satellite based systems for personal wireless applications to the end user will be the focus.

LEOS systems will be less costly to build and deploy than GEOS.

There are two classes of LEOS: *Little* LEOS—those using many small satellites (36 or more for global communications); and *Big* LEOS.[23] (See figure 2-9).

The Federal Communication Commission (FCC) created the distinction between *Big* and *Little* LEOS based on the allocation of frequencies to be used (Little LEOS below one Gigahertz; Big LEOS above one Gigahertz), and services they are authorized to provide. Little LEOS handle data traffic only, e.g., messaging, tracking, and monitoring; Big LEOS can provide global mobile telephone service (similar to cellular and PCS) as well as data services, facsimile, paging, geographic positioning, and other services tailored to users needs.

Little LEOS—The services offered by Little LEOS will primarily operate in *nonreal* time, i.e., store and forward messaging and data. Little LEOS services are scheduled for deployment and operation between 1996 and 2000. The service providers consider emergency and personal communications, law enforcement (vehicle location), environmental monitoring, utility monitoring (power grids), shipping cargo management, etc. as potential markets.

Each Little LEOS system will consist of between 25 and 50 satellites orbiting at about (621 miles) above the earth. One or more earth stations will serve as a gateway to the space-deployed system. The earth stations may be linked to other peripheral message management nodes, which could be linked to conventional wireline or wireless communications networks.

Some regulatory matters, domestic and foreign, are yet to be resolved.

Big LEOS—Big LEOS systems are in the development stage, and have not yet been assigned international frequency allocations, although the FCC has recently granted licenses to three of the five potential service providers.

Big LEOS can provide a wide range of voice and data services, including all of the services provided by Little LEOS, plus cellular- or PCS- like telephone service. Communications can be from mobile or fixed Earth stations. These satellite-linked services are considered to be possible alternatives to expensive land-based wire systems in the remote areas of developing countries. The cost, however, will be high, and international country-by-country regulatory questions may slow global deployment.

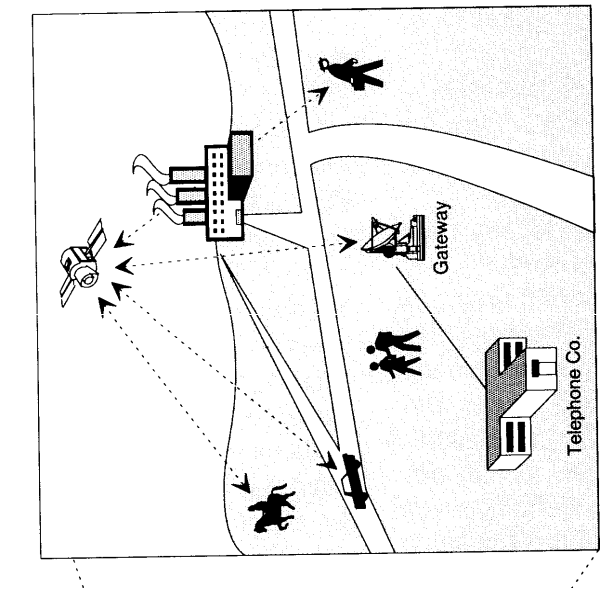
Big LEOs, operating at frequencies above one Gigahertz, will orbit at distances of (310 to 870 miles) above the earth. Communications from a mobile handset would first seek a transmission path to a local terrestrial cellular (or PCS) network (if one exists) for connection to a wireline network. In areas beyond the reach of a cellular network, a direct connection to a satellite station would be made, which would relay the call back to earth for connection with a remote wireline network. After cut-through to the wireline network, a call would be switched as would any other call originating from a cellular, PCS, or conventional switched system.

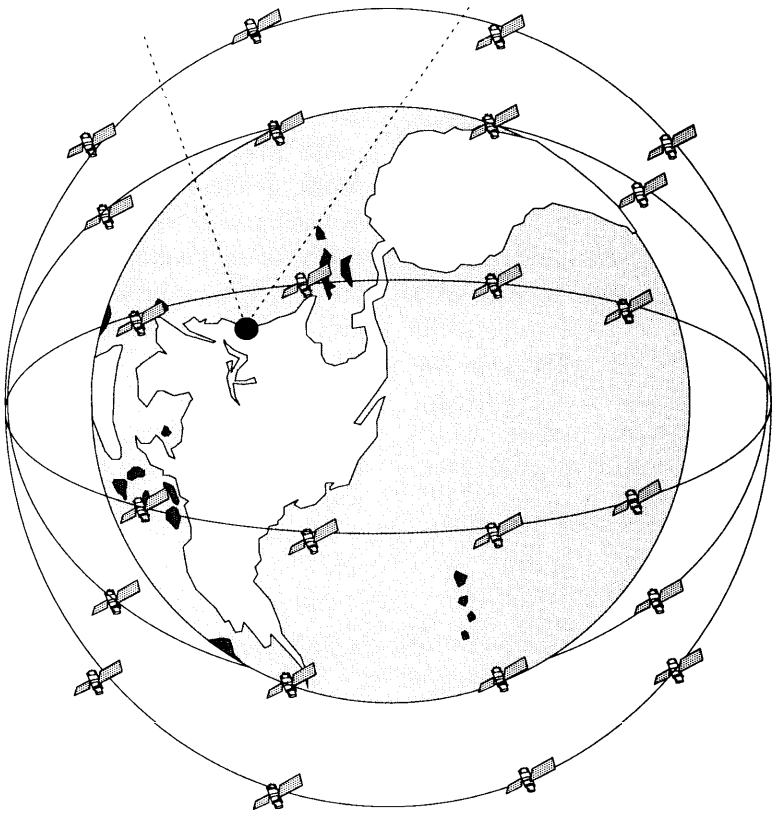
However, Motorola's proposed *Iridium* system[24] would permit callers to make a direct connection from one handset to another through

---

[23] The terms "big" and "little" have little to do with the physical size of the satellites. The primary difference is the radio frequencies that have been allocated to each service. "Little" LEOS will operate at frequencies less than one Gigahertz; "Big" LEOS will operate at frequencies above one Gigahertz. The difference in frequencies affects the nature of the services offered by each of the two LEOS.

[24] Motorola's *Iridium* system would use 66 LEOS orbiting in 11 different planes of 6 satellites each. This would provide worldwide telephone and data communication linked to 15 to 20 Earth stations connected to terrestrial wireline networks. Satellite-to-satellite cross links would be capable of data rates up to 25 Million bits/second (Mbps). Several other companies are proposing similar systems, e.g. Globalstar (Loral and Qualcomm, Inc.), Odyssey (TRW, Inc. and Teleglobe), Ellipso (Mobile Communications Holding, Inc.), ECCO (Equitorial Constellation Communications—Constellation Communications, Inc., Bell Atlantic Enterprises International, and Telecommuniccacoes Brasileiras S.A.). Not all of these systems will offer intra-satellite communications from caller to caller as will *Iridium*.





SOURCE: Federal Bureau of Investigation, 1994.

intrasatellite links. Satellite-to-satellite communication could seriously complicate law enforcement's ability to perform lawful electronic intercepts.

Packet Switched Transmission Technologies

The historical evolution of telephone technology was aimed at optimizing voice communication. Appeals from the fledgling computer users of the 1960s to the telephone companies for better methods of transmitting data from one computer to another were largely ignored. This led the government and the computer industry to seek other means for filling its needs. Thus, two technological cultures developed independently of each other, with little in common between the two and with little interaction among scientists and engineers in both camps.[25]

Today, computers *are* the telephone network, and the fastest growing traffic on telephones networks is data and computer-mediated communications. The *lingua franca* of both telephony and computer communications is the digital transmission mode. Voice, data, video, and images are all transmitted, and for practical purposes, look and are processed the same way. The concept of a National Information Infrastructure (NII) is based on the common ground provided by digital technology that can serve the needs of all users.

While the telephone industry continued to improve the efficiency, quality, and reliability of circuit-connected architecture for voice traffic (which tends to ebb and flow), the computer communication industry developed *packet* technologies to handle the *bursty* (short transactions with periods of no traffic) nature of high-speed computer data.

A number of packet-switched networks were deployed to meet the increasing need for computer communication. Many of these networks were part of a national computer network inspired by the Department of Defense (DOD) in the late 1960s to meet its mission needs.[26] DOD was instrumental in developing packet network technology and packet protocols (the rules for formatting, addressing, and routing the packets within the network). The DOD protocols and routing technology (Transmission Control Protocol/Internet Protocol—TCP/IP) has become a defacto industry standard, and the operating standard for the Internet. The Internet's phenomenal growth and success spawned the vision of a National Information Infrastructure (NII), which appears poised to subsume all telecommunications under its aegis.

Prior to the development and deployment of packet-switched networks, computer users relied on *modems* (modulate/demodulate) for communication over the telephone network. Modems convert the digital signals produced by a computer to electrical signals (analog signals) that look and behave in the telephone network as though they were sounds or spoken words. At the receiving modem, the *analog* electrical signals are converted back to digital form before re-entering the receiving computer. Modem technology is still a common means for communicating between computers over the Public Switched Telephone Network (PSTN). However, the speed of modem transmission is relatively slow and thus limits their usefulness for high-speed, broadband applications, e.g., video and images.

A packet-switched network can send information over several different routes (like choosing alternative interconnected highways) to reach a destination. Data placed in packets (segments of

[25] Even today the schism between the two industries remains evident. The two cultures continue to exist, with different language and different perspectives on communications, although both use common digital technology and are being forced to act as one, if ever so reluctantly.

[26] A number of regional networks and Internet service providers have appeared to meet the increasing demand. Many of these entities lease lines from the Public Switched Telephone Network (PSTN), although the Internet operates independently of the PSTN.

data and routing information) containing special control information (source and destination address) are sent along any route within the network that happens to be available that leads to the addressee.[27] Because of the random nature of the route to the destination taken by packets, they arrive at different times and out of order, although each contains only a portion of the data or message sent by the originating computer. Packets must be assembled and disassembled at the receiving end and put in the same order or sequence as they were sent.

Intervening years have brought increased demand for switched broadband networks to handle the high capacities needed for video, images, and data. In response to this the telephone industry has attempted to recoup the business it lost to private networks and information service providers by improving its computer communication services.

In 1976, the telephone industry adopted an international packet switching standard designated *X.25*, a relatively slow transmission service.[28] Since then, Switched Multimegabit Data Service (SMDS) and Frame Relay (a technology that uses packets of variable payload length)[29] have been introduced. Both SMDS and Frame Relay are precursors of what the telephone industry considers to be its technology backbone of the future—the Asynchronous Transfer Mode (ATM)

Asynchronous Transfer Mode (ATM)

ATM is a *fast packet switching* technology, i.e., it provides fast processing power that can keep up with the increased bandwidth (volume) available with very fast transmission systems over optical fiber, which are required for video. ATM is flexible enough to support voice, video, images, and data. It is a scaleable technology, i.e., it can be used to link a few computers in an office setting, it can serve a *campus* setting, like Capitol Hill, it can be expanded to cover an area the size of Washington, DC., or it can work in a national network, as proposed for the National Information Infrastructure. It has the added advantage of being accepted and supported by both the computer industry and the telecommunications industry.

ATM has two distinguishing features:

1. It is *cell-based*. Instead of variable-length frames, as used by Frame Relay and other packet networks (sometimes several thousand bytes, which contain 8 bits of binary information), ATM uses fixed-length cells. (See figure 2-10.)
2. ATM is *connection-oriented*, i.e., every cell in the ATM transmission travels over the same route. The network path, or *virtual circuit*, is designated during call setup by information contained in the cell header. The header in the ATM cell contains the information a network needs to relay the cell from one network node (switching point) to the next over the pre-established route.

ATM *connections* are sets of routing tables retained in an ATM switch, which are matched with the address contained in an ATM cell header. ATM addresses, unlike a geographically locatable Directory Number (DN) or a TCP/IP packet, only have meaning for locating one point (node) in an ATM net to the next node.

Each ATM switch is provided with a set of lookup tables (computer database), which identify an incoming cell by header address, route it through the switch to the proper output port, and overwrite the incoming address with a new one that the next switch along the route will match with an entry in its routing table. Thus, the message is passed along from switch to switch, over a prescribed route, but the route is *virtual*, since the switch carrying the message is dedicated to it only while the cell is passing through it.

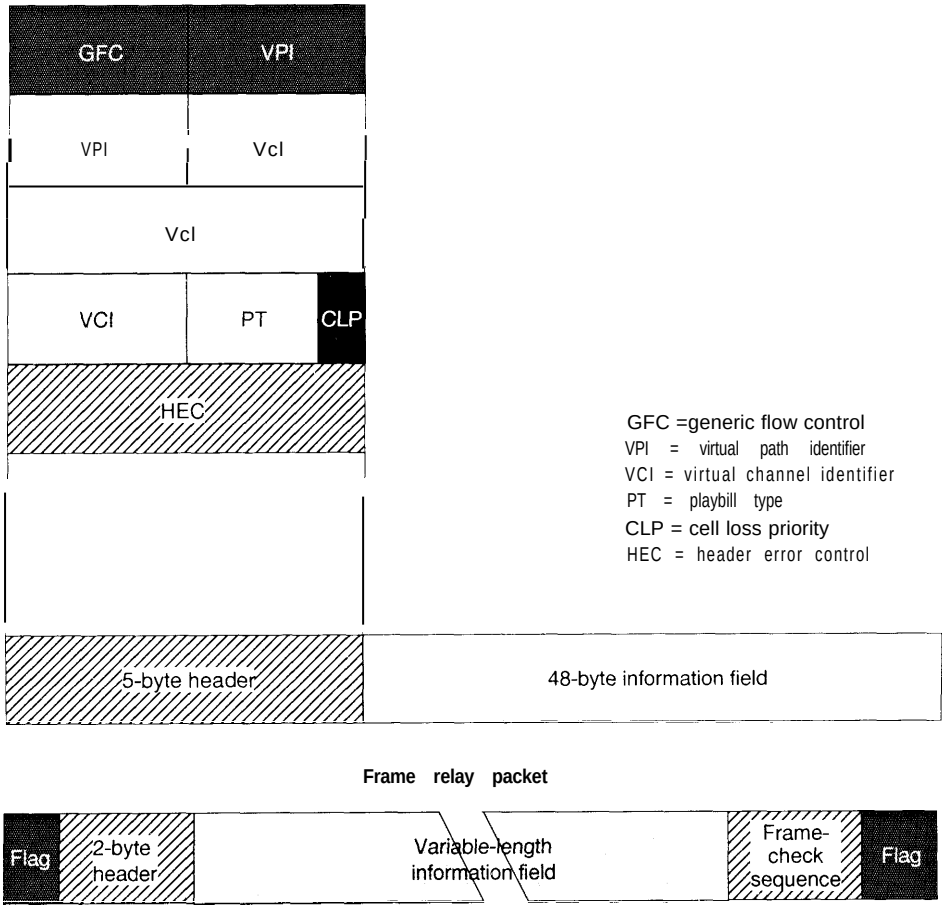
---

[27] Packets have been compared to envelopes used for traditional mail. The data or information in the packet data field is like the writing on paper, and the numerical address of the computer to which it is sent that is contained in the packet header is like the address on an envelope.

[28] X.25 packet switching carries a relatively low data rate of approximately 9.6 kilobits/second.

[29] Frame Relay is not based on fixed-length data frames, it uses flags in the header and trailer to indicate the beginning and end of frames.

FIGURE 2-10: ATM and Frame Relay Cell Structure



Key' GFC=generic flow control, VPI=vlrtual path identifier, VCI=virtual channel identifier; PT=playbill type, CLP=cell loss priorly, HEC=header error control

SOURCE James Lane, IEEE Spectrum, p 43, February 1994

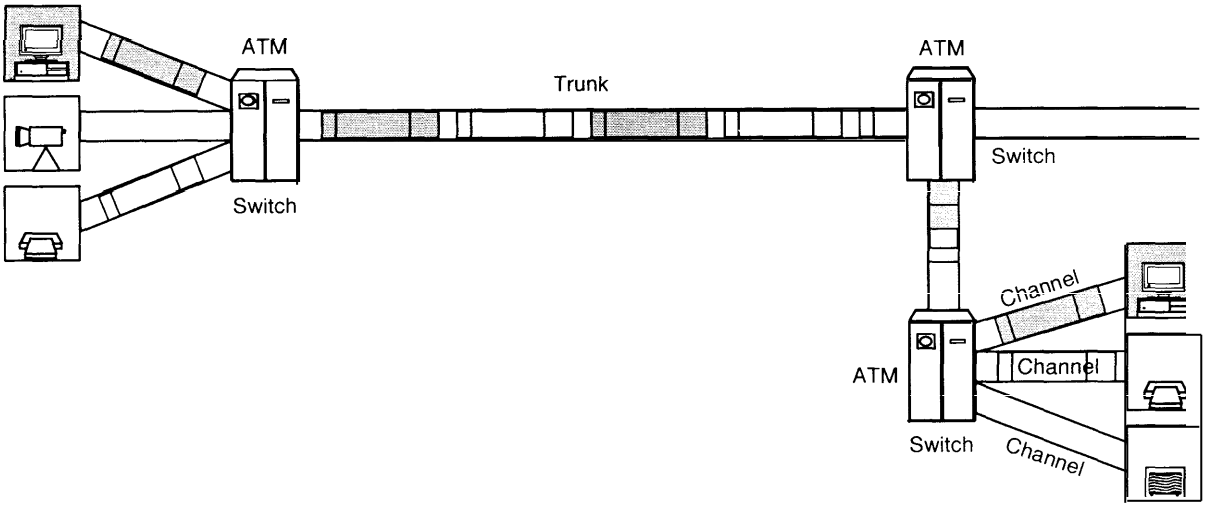
The address in the header of an ATM cell contains two fields:

1. Virtual Path Identifier (VPI); and
2. Virtual Channel Identifier (VCI).

The two-part addressing scheme allows the network to designate major trunks between locations, and identify the individual circuits (channels) within the trunk. A virtual path may consist of several virtual channels. Thus, the VPI might represent a trunk between two cities. The VCIs might represent individual calls. Switching equipment along the network can route all the calls on the basis of just the VPI without having to query the rest of the address (VCI) until the trunk gets to the final location, where the individual calls are distributed to their destinations. (See figure 2-11.)

Implications for Electronic Surveillance—If ATM becomes the enabling technology for the nation's next generation of multimedia networks (the NII) as some foresee, interception of electronic communication will become more difficult. Packet networks will require a substantially dif-

FIGURE 2-11: ATM Multi-Media Switching Network



SOURCE Off Ice of Technology Assessment, 1995

ferent approach to surveillance than used for today's digital telephony. Since the address is an integral part of the packet that contains the message data as well, it will be necessary to develop means to insert *hooks* into the packet header to identify the sender and the intended recipient.

Packets in *connectionless services, e.g.,* Internet (TCP/IP), and Frame Relay, have destination addresses embedded in the packet that are identifiable with a physical location and/or an individual. A packet may travel any number of alternate routes in reaching its destination. Since information is segmented into variable length packets, connectionless routing can result in a packet containing part of the message that is sent before another, may reach its destination after the second or later packets that are sent. Connectionless packets must be reassembled in proper order to make sense of the message. Once a message is sent by an intercept subject, random routing will complicate the process of identifying the packets—and only the packets—that are authorized to be lawfully intercepted until they reach their destination.

ATM establishes a virtual circuit between ATM switches (but not physical connections as used in the Public Switched Telephone Network) that routes each ATM cell over the same trunk and channel. Many different calls (video, voice, images, data) in addition to that of the intercept subject or his or her correspondent maybe moving over the same routes simultaneously and/or intermittently. The route in the header address is overwritten with a new address at each ATM switch, which is translated from the switch route lookup table. The unique routing protocol of ATM will require new approaches to message identification and verifications and will complicate trap and trace and pen register procedures.

Internet (TCP/IP) and Frame Relay packets can be sent over ATM networks, although ATM cannot recognize the embedded packet addresses in the headers. ATM incorporates the entire TCP/IP or Frame Relay packet into an ATM cell and readdresses the cell according to the ATM routing protocol. At the point of termination, the ATM envelope is stripped away and the TCP/IP packets are assembled for processing by the recipient. This may further complicate the identification and association of a *call* from or to the subject of a lawful electronic intercept. Moreover, there is currently a market in redirecting TCP/IP traffic, or changing a sender's address to an anonymous ad-

dress. Some of these services are based in foreign jurisdictions, thus possibly complicating the legal procedure for identifying communications from or destined for a lawful intercept subject.

In addition to the technical difficulty in dealing with packet-based communication in general, and ATM networks in particular, the legal requirements for establishing a lawful electronic intercept may be more difficult. The isolation of an intercept subject's outgoing and incoming traffic according to the strict requirements that assure the privacy of other communicants may be more difficult. *Minimization*, i.e., screening or filtering nongermane information from the intercepted communication, also may be more complicated.

Appendix B: Electronic Surveillance Requirements Keyed to P.L. 103-414

B

REQUIREMENT 1

A) Law enforcement agencies require access to the electronic communications transmitted, or caused to be transmitted, to and from the number, terminal equipment, or other identifier associated with the intercept subject throughout the service areas operated by the service provider served with a lawful authorization. Law enforcement agencies also require access to generated call-identifying information necessary to determine the calling and called parties. Law enforcement agencies will coordinate delivery of these communications with the service provider in accordance with Requirement 3(A) *infra* for each service area. (Sec. 103(a)(1), Sec. 103(a)(2))

B) Law enforcement agencies require real-time, full-time monitoring capability for interceptions. (Sec. 103(a)(1))

C) Law enforcement agencies require telecommunications carriers to make provisions for implementing a number of simultaneous interceptions. (Sec. 103(a)(1))

D) Law enforcement agencies require telecommunications carriers to expeditiously provide access to the communications of the intercept subject. (Sec. 103(a)(1))

REQUIREMENT 2

Law enforcement agencies require:

1) information from the telecommunications carrier to verify the association of the intercepted communications with the intercept subject, and
2) information on the services and features subscribed to by the intercept subject prior to and during the intercept implementation. (Sec. 103(a)(2))

REQUIREMENT 3

A) Law enforcement agencies require telecommunications carriers to transmit intercepted communications to a monitoring facility designated by the law enforcement agency. (Sec. 103(a)(3))

B) During the intercept period, law enforcement agencies require that the reliability of the services supporting the interception at least equals the reliability of the communications services provided to the intercept subject. (Sec. 103(a)(3))

C) Law enforcement agencies require that the quality of service of the intercepted transmissions forwarded to the monitoring facility

comply with the performance standards of the telecommunications carriers. (Sec. 103(a)(3)

REQUIREMENT 4

Law enforcement agencies require the intercept to be transparent to all parties except the investigative agency or agencies requesting the intercept and specific individuals involved in implementing the intercept capability. Law enforcement agencies require the implementation of safeguards to restrict access to intercept information. (Sec. 103(a)(4))

Appendix C: Related OTA Reports for Further Reading

C

- U.S. Congress, Office of Technology Assessment, *Critical Connections: Communication for the Future*, OTA-CIT-408 (Washington, DC: U.S. Government Printing Office, January 1990)
- U.S. Congress, Office of Technology Assessment, *The 1992 World Administrative Radio Conference: Technology and Public Policy*, OTA-TCT-549 (Washington, DC: U.S. Government Printing Office, May 1993)
- U.S. Congress, Office of Technology Assessment, *Advanced Network Technology*, OTA-BP-TCT-101 (Washington, DC: U.S. Government Printing Office, June 1993)
- U.S. Congress, Office of Technology Assessment, *Protecting Privacy in Computerized Medical Information*, OTA-TCT-576 (Washington, DC: U.S. Government Printing Office, September 1993)
- U.S. Congress, Office of Technology Assessment, *Information Security and Privacy in Network Environments*, OTA-TCT-606 (Washington, DC: U.S. Government Printing Office, September 1994)
- U.S. Congress, Office of Technology Assessment, *Wireless Technology and the National Information Infrastructure*, (to be released Summer 1995)

Glossary

Access
The technical capability to interface with a communications facility, such as a communications line or switch, so that law enforcement can monitor and receive call setup information and call content.

Actual Capacity
That portion of the Maximum Capacity simultaneously required to conduct electronic surveillances at or before a specified date in a given switch as indicated by the Attorney General for all government agencies authorized to do surveillance.

Advanced Intelligent Network (AIN)
A system of interrelated computer-based components linked to a switched or wireless telecommunications network that provides a framework for services, e.g., call forwarding, credit card authentication, personal identification numbers, speed dialing, voice dialing, etc.

Base Station
The common name for all of the radio equipment located at a single site for serving one or several cells.

Call
Any wire or electronic signaling information generated by a human or a computer acting as an agent for a human to set up a physical or virtual connection to transit information to another or multiple users (humans and/or computer processes).

Call Content
The same as "contents" as defined in 18 U.S.C. 2510 (8) and with respect to any electronic communication, includes any information concerning the substance, purport, or meaning of that communication.

Call Content Channel (CCC)
The link between the surveillance switch and the law enforcement agency that carries the call content. The CCC may be a switched connection or a dedicated path through the Public Switched Telephone Network (PSTN), e.g., on a private line.

Call Data Channel (CDC)
The interface between the surveillance switch and the law enforcement agency that carries the call set-up data. The CDC may be a switched connection or dedicated path through the Public Switched Telephone Network (PSTN) or may be separate from the PSTN, e.g., via a private line or a packet switched network.

Call Setup Data
Includes all of the setup and call release information received and interpreted by the surveillance switch as a regular part of processing the call as defined in applicable standards and specifications for the services being provided. For example, this includes the initial digits dialed to access an Interexchange Carrier (IC) but may not include those dialed via Dual Tone Multi-Frequency (DTMF) after connection with the IC.

Call Setup Information
When used with respect to any electronic communication, the information generated during the establishment of communications or transmission of a protocol data unit such as a datagram, that identifies the origin and destination of the call. For

voice communications, this information is typically the electronic pulses, audio tones, or signaling messages that identify the numbers dialed or otherwise transmitted, or caused to be transmitted, by the intercept subject. It also includes incoming pulses, tones, or messages that identify the number of the originating instrument, device, or user. For data services, this information is typically the source (calling) address and destination (called) address contained in fields of the data unit, such as in the header of a frame or packet.

Calling Features Indicator
The authorization and activity status of the Mobile Switch features, including call forwarding (unconditional, busy, no answer), call waiting, three-way calling, and call delivery.

CDMA
Code-Division Multiple Access.

Central Office
In telephone operations, the facility housing the switching system and related equipment that provides telephone services for customers in the immediate geographical area.

DTMF
Dual tone, multi-frequency, i.e., push button dialing.

Electronic Communications
The same as defined in 18 U.S.C. 2510 (12), any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic photo-electric, or photo-optical system, etc. The term includes "wireless communication," as defined in 18 U.S.C 2510 (1).

Electronic Serial Number
A coded serial number assigned by the manufacturer to the mobile unit.

Electronic Surveillance
The statutory-based process and the associated technical capability and activities of law enforcement agencies related to the interception and monitoring of electronic communications.

Handoff
Occurs when a subscriber travels from one service area to another while a wireless call is in progress.

Home Location Register (HLR)
The location register to which a user identity is assigned for record purposes, such as subscriber information (e.g., Electronic Serial Number, Directory Number, Profile Information, Current Location, Validation Period). The HLR may or may not be located within, and be indistinguishable from, a Mobile Switching Center (MSC). A HLR may serve more than one MSC and the HLR may be distributed over more than one physical entity.

Home Service Area
The service area in which a customer has subscribed to receive service.

Intercept Subject
Person or persons identified in the lawful authorization and whose incoming and outgoing communications are to be intercepted and monitored.

Interface
A shared boundary or point common to two or more similar or dissimilar command and control systems, subsystems, or other entities against which, or at which, or across which useful information takes place.

Local Exchange
An exchange where subscribers' lines are terminated.

Local Switch
A switch that connects one customer's line to another customer's line, or to a facility that goes to another switching system, i.e., a trunk.

Maximum Capacity
That switch capacity (in terms of the number of simultaneous surveillances and the number of simultaneous monitorings) that cannot be exceeded in a switch without revision of its generic software.

Mobile Identification Number
An identification number assigned by the service provider to a subscriber.

Mobile Station (MS)
The interface equipment used to terminate the radio path at the user. It provides the user the ability to access network services.

Mobile Switching Center (MSC)
An automatic switching system that constitutes the interface for user traffic between the cellular network and public switched networks or other MSCs in the same or different cellular networks.

Monitoring
The process of capturing information, either call content or call set-up information or both, in real time during he processing of a call. (This does not include nonreal time access to stored data such as billing records for previous calls or subscription parameters).

Multiple Agency Distribution
The capability to provide multiple surveillances of a given access to a target to satisfy the needs of more than one government agency by some appropriate means.

Multiplex (MUX)
Use of a common channel to make two or more channels. This is done either by splitting of the common channel frequency band into narrower bands, each of which is used to constitute a distinct channel (frequency division multiplex), or by allotting this common channel to multiple users in turn, to constitute different intermittent channels (time division multiplex).

Packet Switching
A system whereby messages are broken down into smaller units called packets that are then individually addressed and routed through the network.

Pen Register
A device that records or decodes electronic or other impulses that identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached. Pen Register is an archaic name that survived the transition from pulse dialing to touch-tone dialing. The recording device is now called a "Dial Number Recorder" (DNR). The term does not include a device used by a service provider for billing, or recording incidental to billing, for communications services, or any device used by a service provider for cost accounting in the course of business.

Private Branch Exchange (PBX)
Small local telephone office, either automatic or manually operated, serving extensions in a business complex and providing access to the public switched telephone network.

Remote Switch
A switch associated with, and controlled by, an exchange in a different location (host switch). Host switches can serve several remote switches, and are connected to the remotes with facility links.

Roaming
When the subscriber initiates or receives a call in other than his or her home service area.

Service Profile Information
The set of features, capabilities, and/or operating restrictions associated with a subscriber, e.g., account code digits, alternate billing digits, etc.

Service Switching Point (SSP)
A specially designed switch that contains Advanced Intelligent Network (AIN) switching capabilities.

Stored Program Control Point (SPCP)
A computer component that stores many of the intelligent functions of an Advanced Intelligent Network (AIN).

Surveillance
The process of maintaining watch on a target, on behalf of a single law enforcement agency, for the occurrence of originating or terminating calls that must be monitored or for any other activity that must be recorded, such as administrative changes to the service parameters.

Surveillance Switch
The circuit switch which identifies calls made from or to the target and which performs surveillance. This is normally the local exchange (or end-office) serving that target.

Tandem Switch
A switch that connects trunks to trunks.

Target
An identifiable origination or termination of a telecommunications call. The most common identifier is the telephone number (or "DN") that a call is made to or from, but other identifiers may also be used.

TDMA
Time Division Multiple Access

Transmission
The act of transferring a sign, signal, writing, image, message, sound, data, or other form of intelligence (information) from one location to another by a wire, radio, electromagnetic, photoelectronic, or photo-optical system.

Transparency
The circumstances wherein the parties to a communication and unauthorized individuals (i.e., individuals who are not involved in implementing and maintaining the intercept) are unaware of ongoing electronic surveillance.

Trap and Trace Device
A device that captures the incoming electronic impulses that identify the originating number of an instrument or terminal from which electronic communication is transmitted.

Trunk
A circuit between two ranks of switching equipment in the same office, or between different switching centers or different central offices.

Verification
The process whereby law enforcement can adequately demonstrate to a judge or jury that the number or other identifier (e.g., telephone number, electronic mail address) targeted for interception corresponds to the person or persons whose communications are being intercepted.

Visitor Location Register (VLR)
The location register other than the Home Location Register (HLR) used by a Mobile Switching Center (MSC) to retrieve information for handling of calls to or from a visiting subscriber. The VLR may or may not be located within, and be indistinguishable from, an MSC. The VLR may serve more than one MSC.