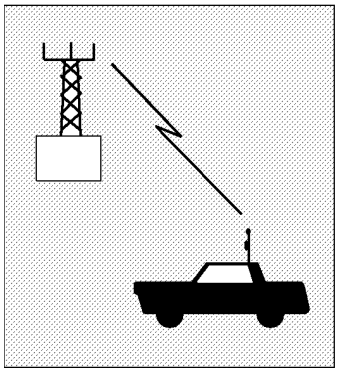
Summary and Discussion 1

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.

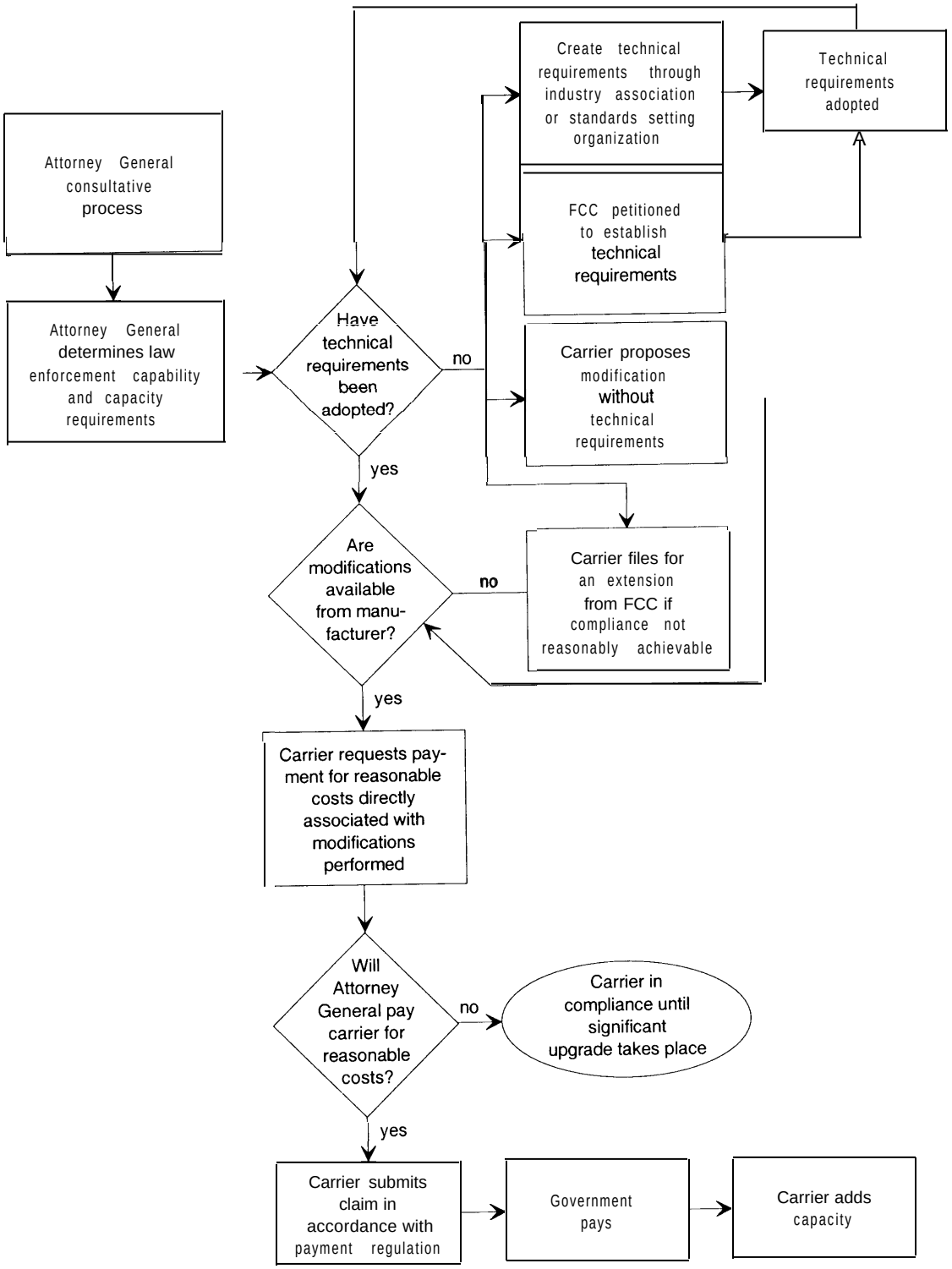
Within 180 days after the Attorney General publishes the capacity notifications, service providers must provide statements that identify those areas where the carrier does not have the capacity to simultaneously accommodate the types of surveillance required. (See figure 1-2.)

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-

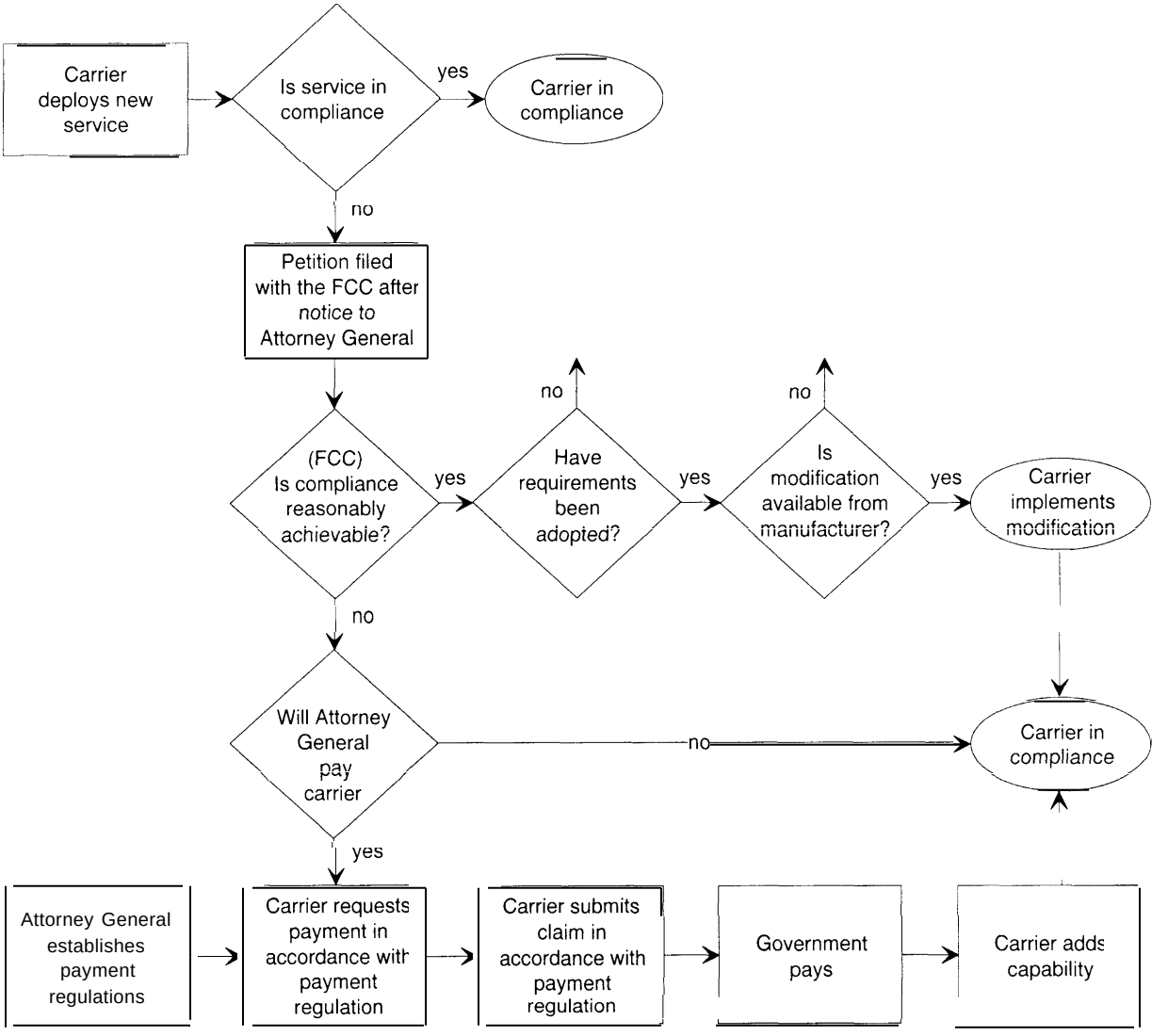
[8] A Common Carrier is a company that furnishes public telecommunications facilities and services, e.g., a telephone or telegraph company. A Common Carrier cannot control message content.

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



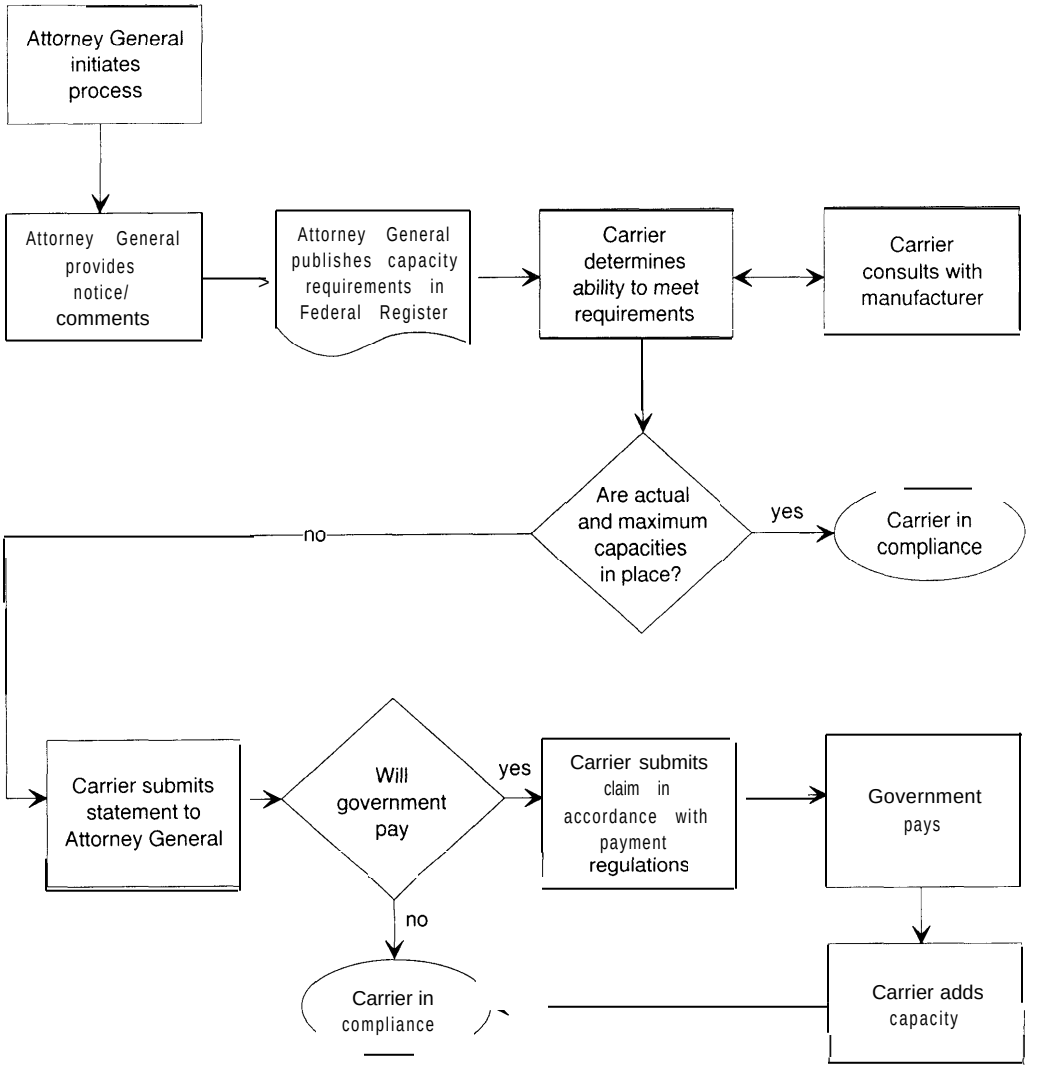
SOURCE Federal Bureau of Investigation, 1995

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

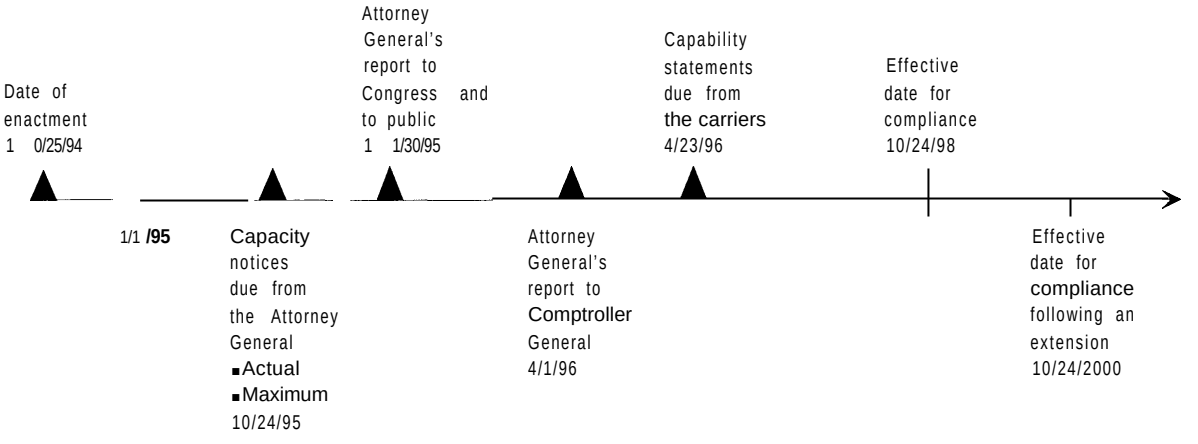


SOURCE Federal Bureau of Investigation, 1995

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

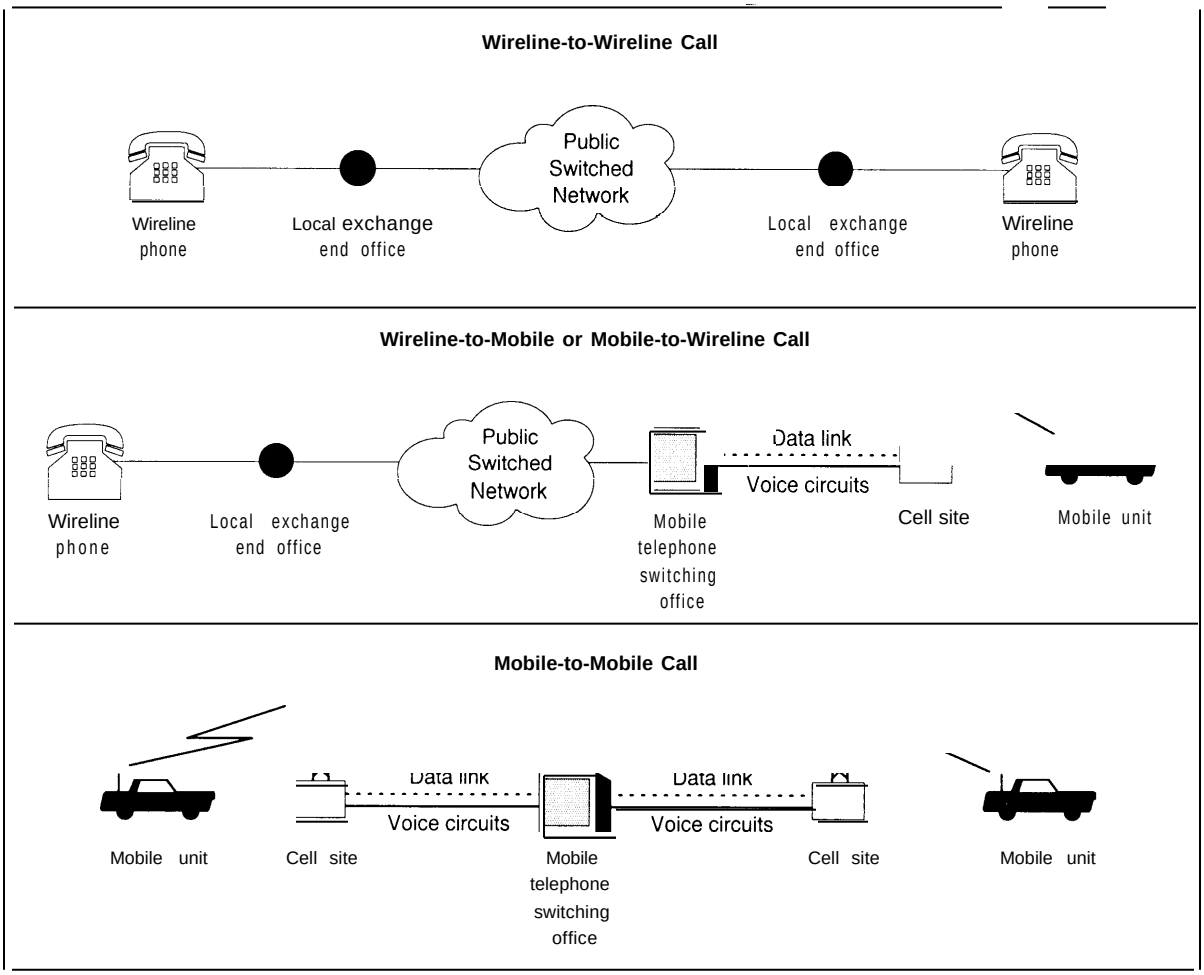
Requirements for accessing call setup information and call content apply to both wireline and wireless mobile communications. A mobile customer can move freely about a home service area and beyond into the service area of another mobile carrier. A service provider's network may cover a local area, a 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

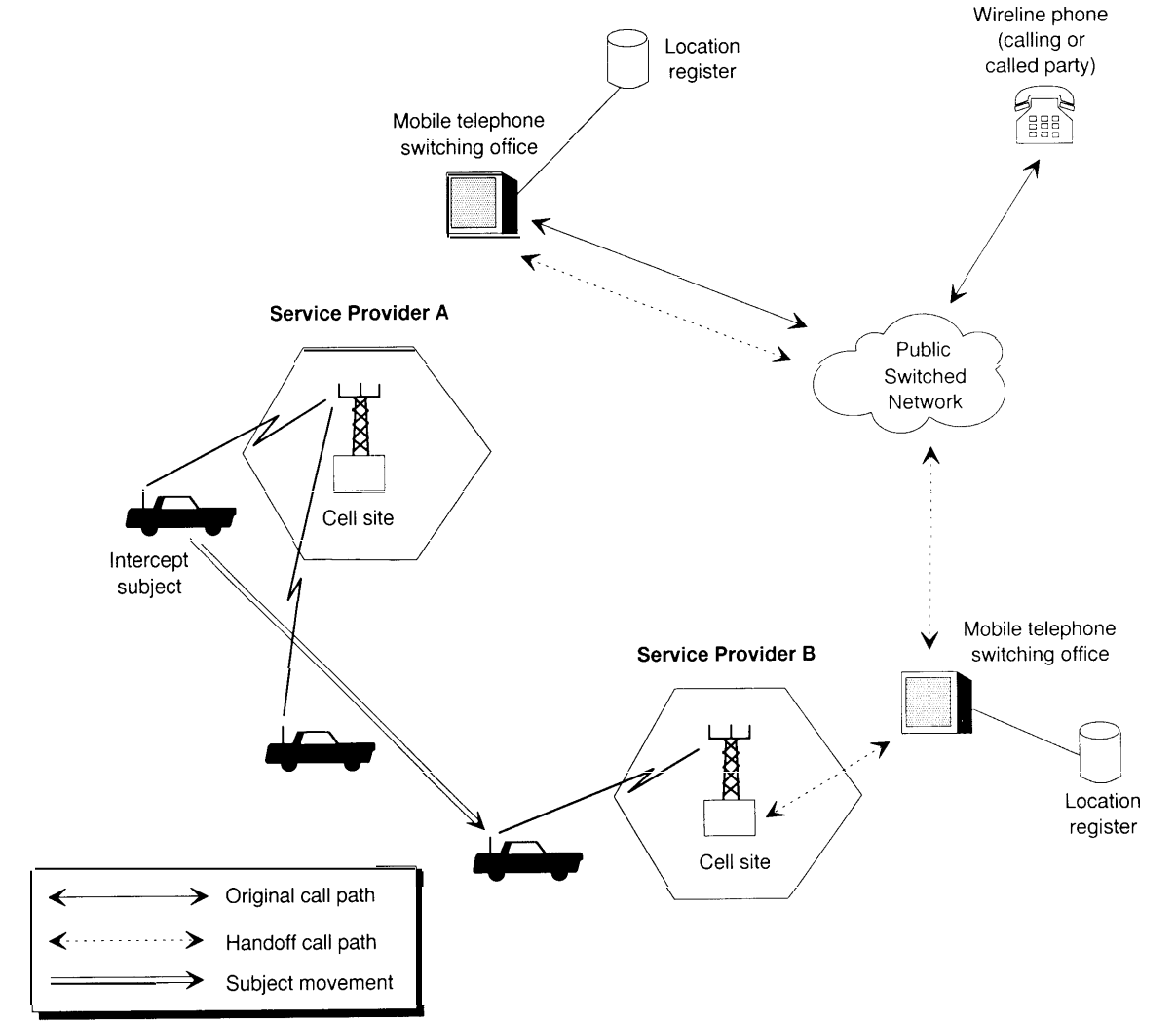
area are registered as visitors in the new service. In those instances, information about the caller's unique Electronic Serial Number (ESN) and Mobile Identification Number (MIN) and other authentication, validation, and routing information are automatically exchanged between the location registers (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)

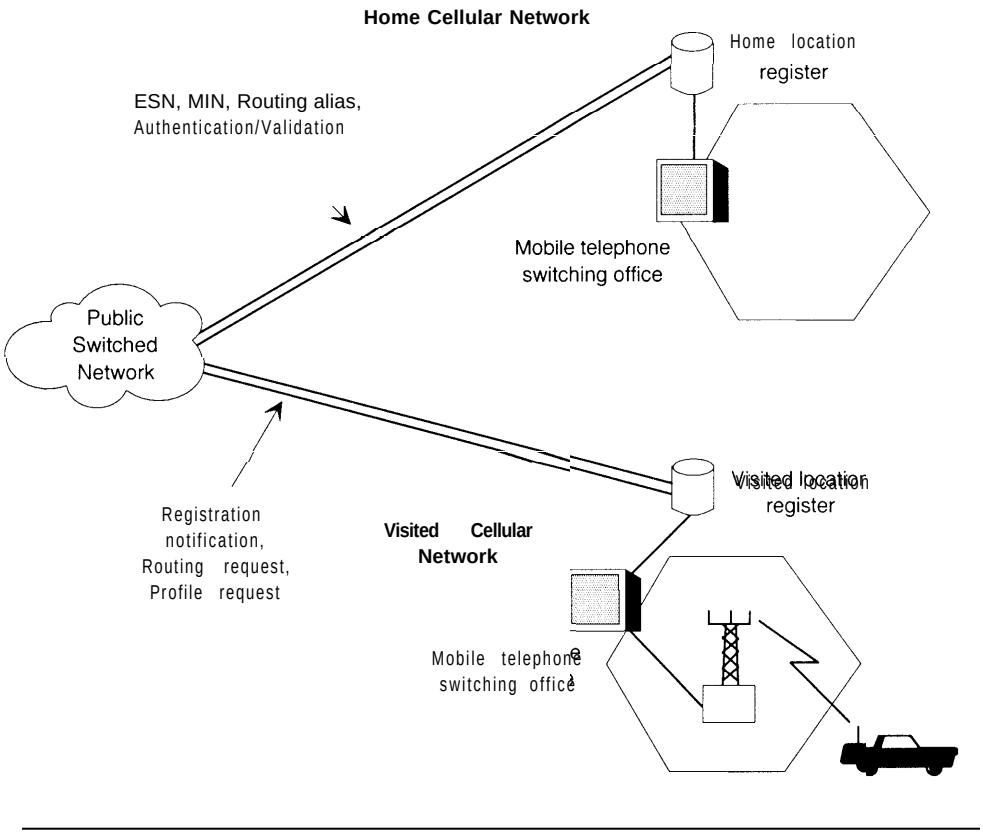


SOURCE Federal Bureau of Investigation, 1994.

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.