

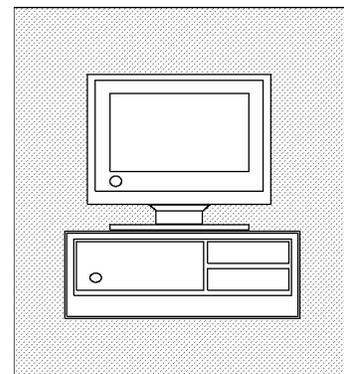
Technical Aspects of Electronic Surveillance¹ 2

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.

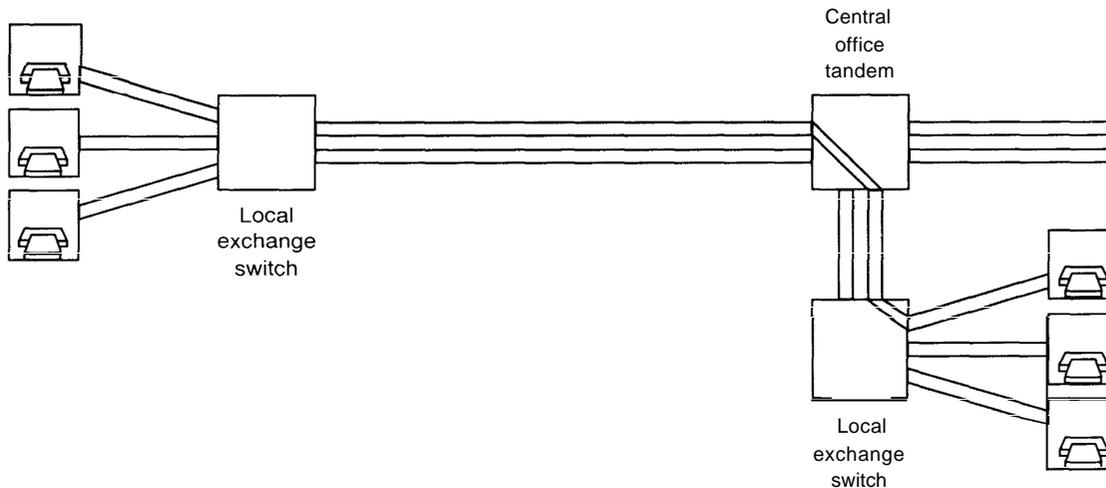
⁴ Id at table 5.

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 Hungry 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 Office 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.

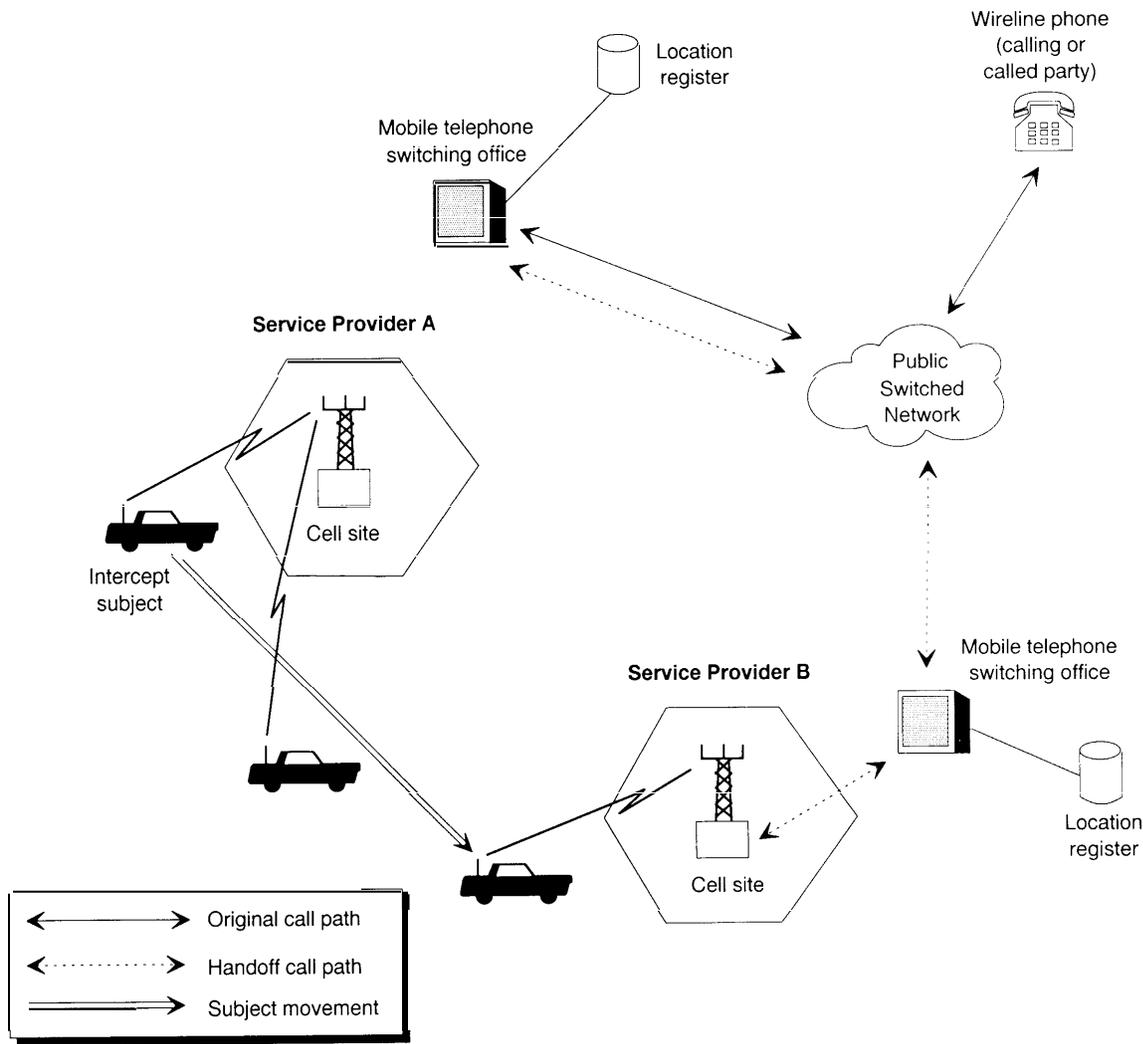
Multiplexing can increase the normal speed of transmission from thousands of bits per second (kbs) to 1.544 million bits per second (Mbs) for T1 and 45 Mbs at the T3 rate. Because multiplexing breaks the continuity of the signal in the transmission phase, it places an additional degree of difficulty 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, im-

bedded 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 carrier's 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.

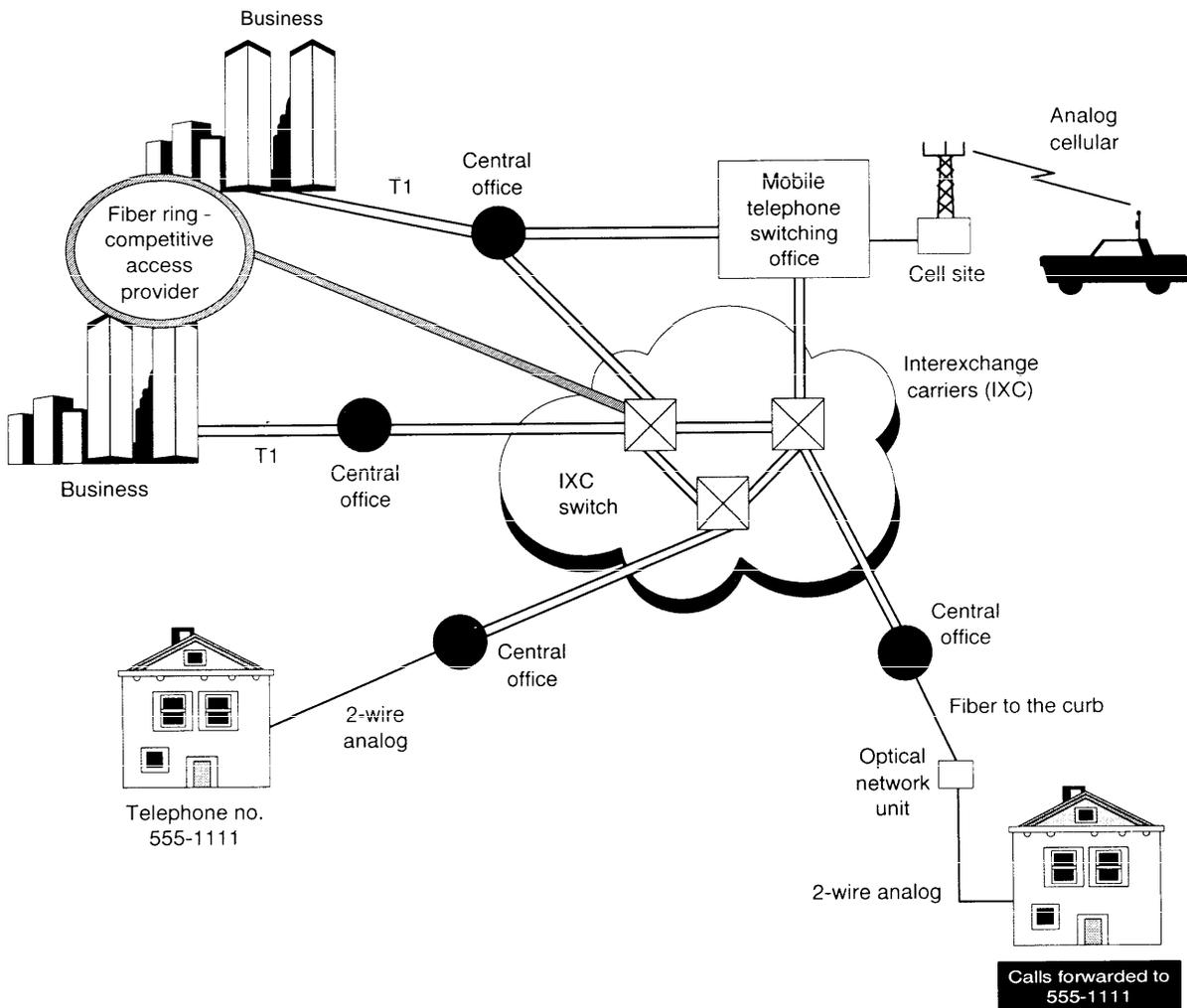
mitted to a designated law enforcement monitoring facility. However, access to the intercept will be controlled by the service provider and not the law enforcement agency. Transmission of intercepted communications must satisfy the following guidelines:

- 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

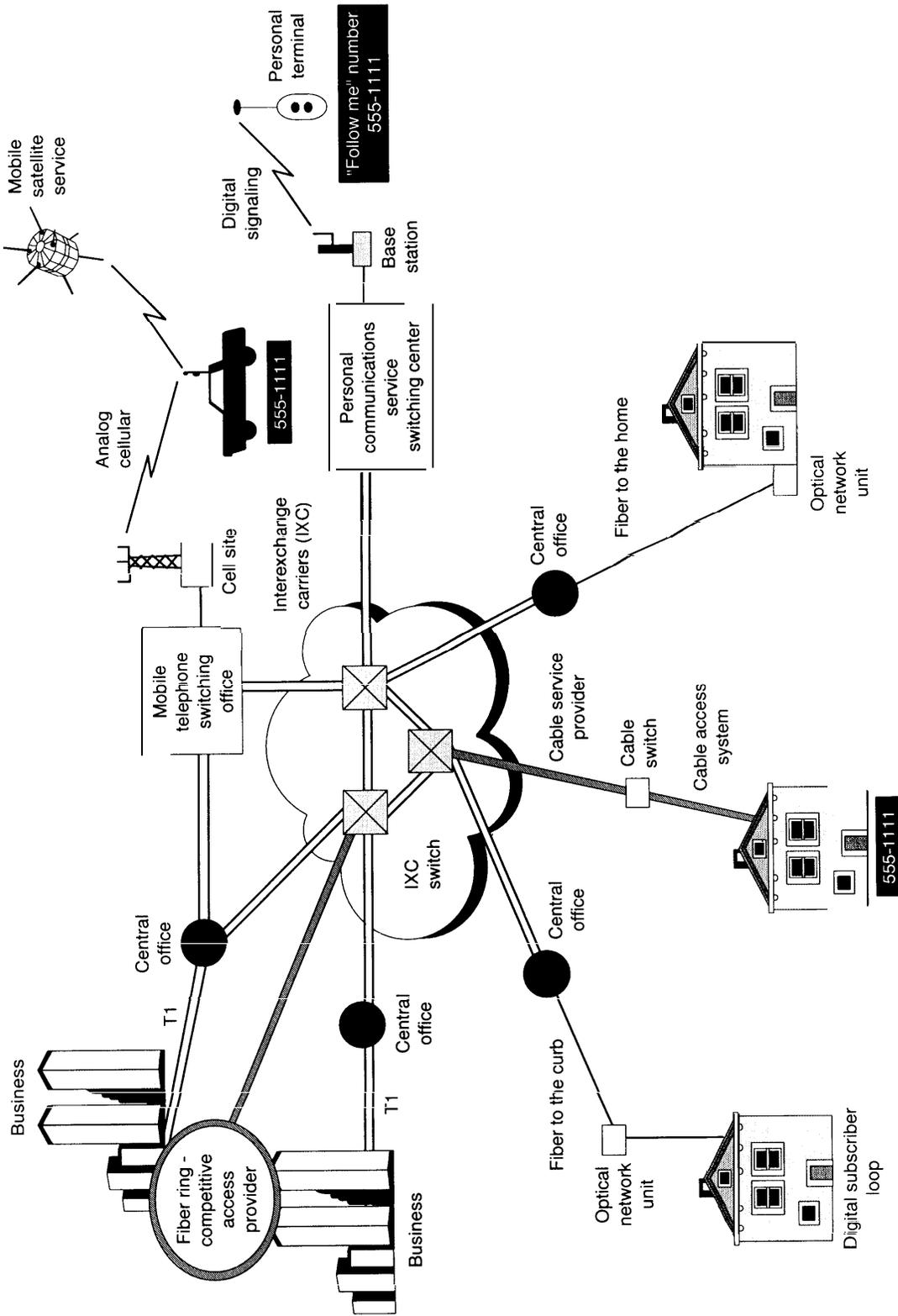
limited by the imagination of the systems engineers and developers and the acceptance of the new applications in the marketplace. Faster transmission systems and computer networking will lead to advanced systems that can leverage the bandwidth into currently unforeseen applications. The vision of a National 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 land-line 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 affect 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 data, 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 data, 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 channeled 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:

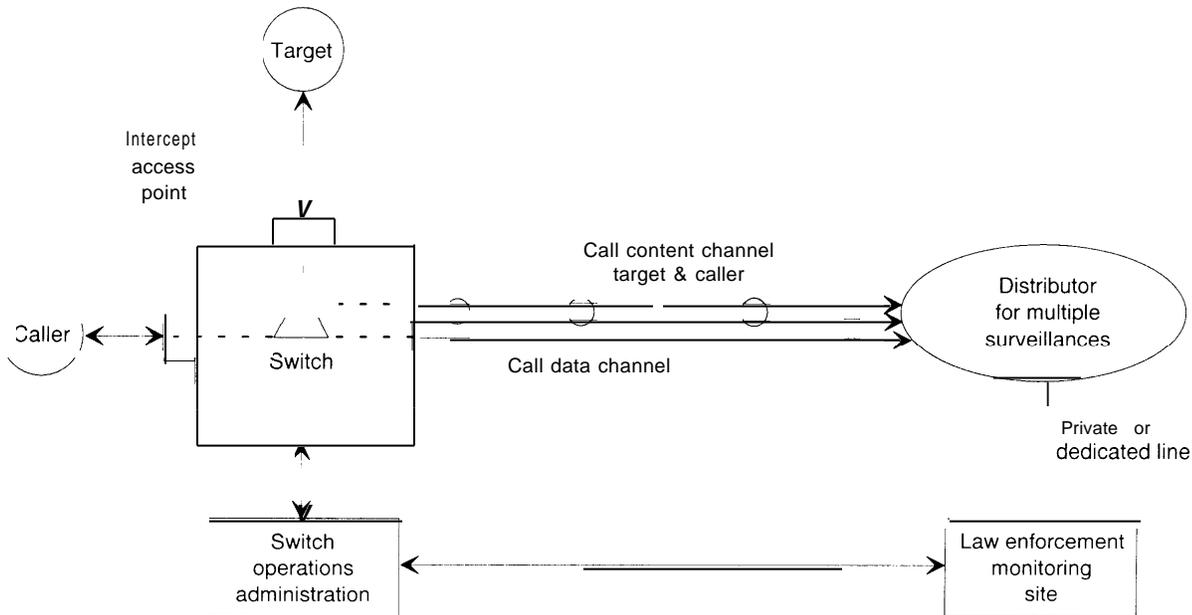
- **Basic Access**—composed of two 64 kbs B-channels (for voice, data, or images) and one 16 kbs D-channel for signaling; and
- **Primary Rate**—operates at a rate of 1.544 Mbs (million bits per second), composed of 23 B-channels of 64 kbs each, and one 16 kbs D-channel for signaling.

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 en-

forcement 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, therefore 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 (Intrasytem 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

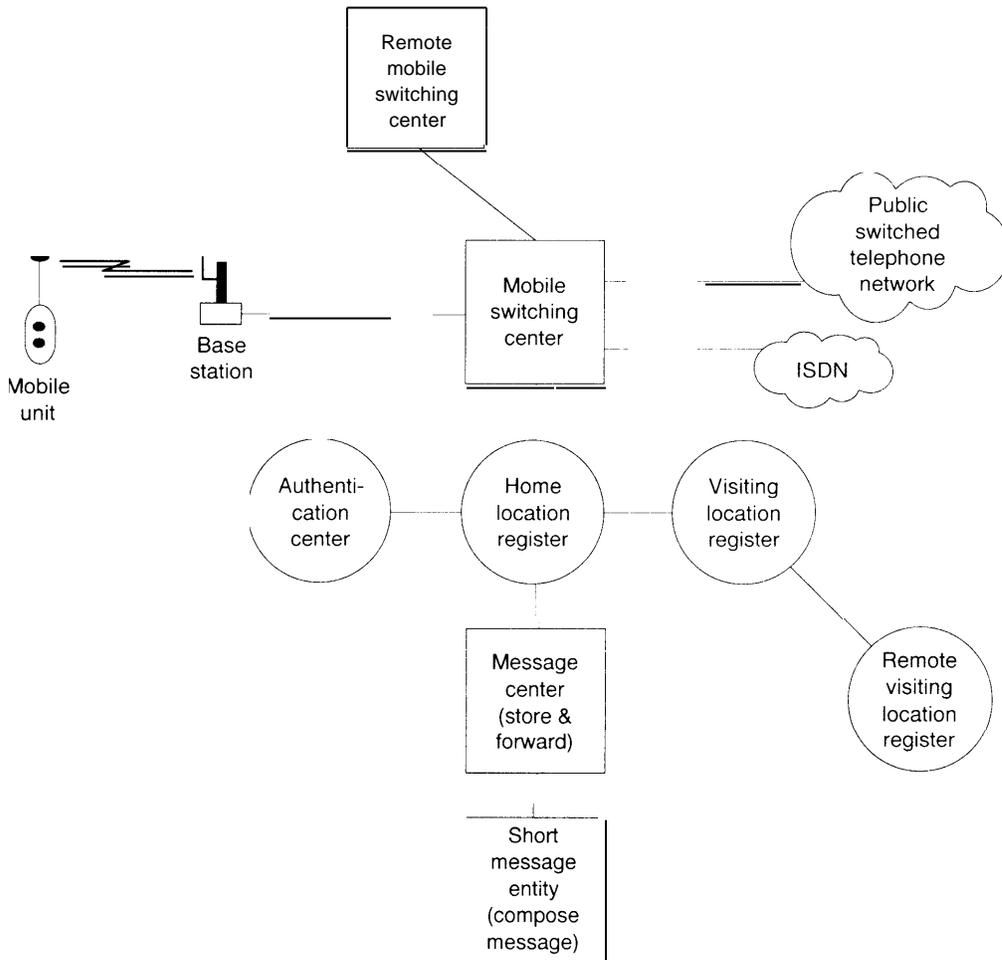
Cellular radio communication may be either analog or digital. The radio components of most of today's cellular networks are analog-based, but many of the carriers are slowly switching from analog systems to digital systems in order to increase the capacity, offer a wider choice of services, reduce fraud,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

¹⁰Roaming 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 subject's 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 VLR 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.

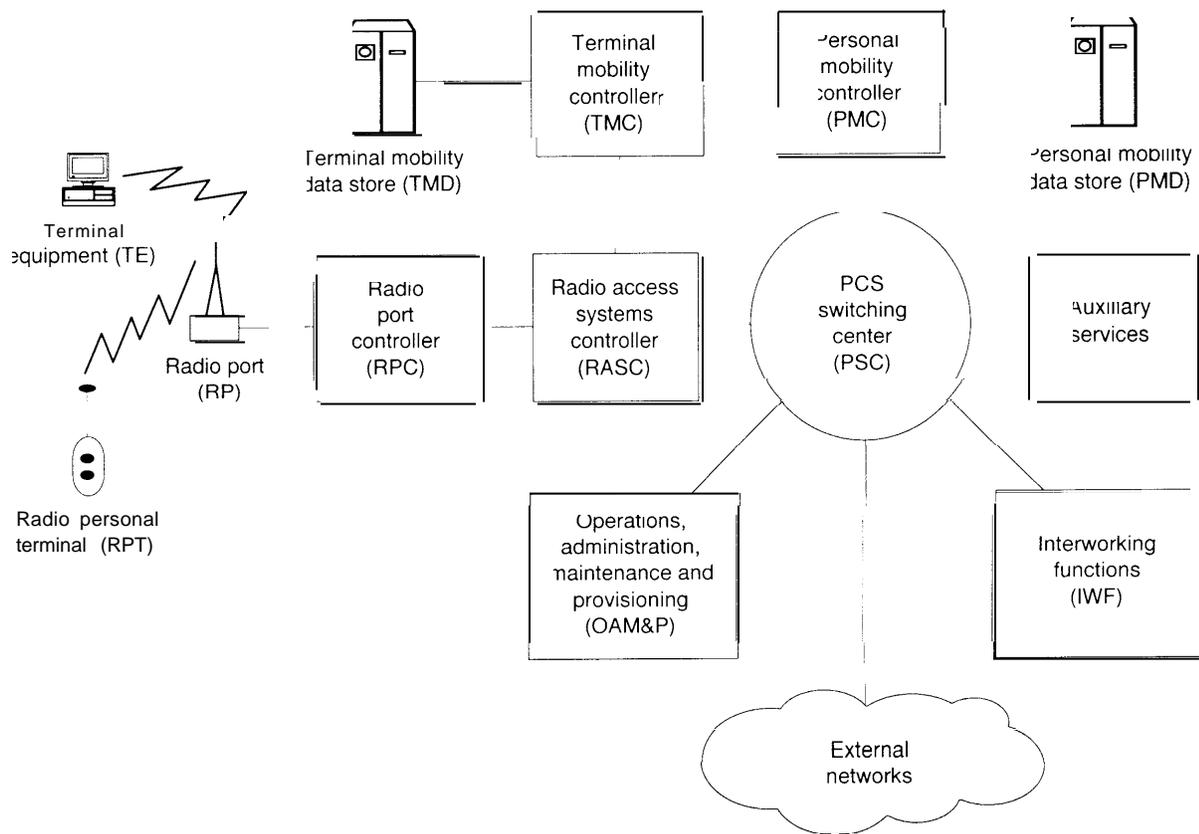
The major difference between the features offered by cellular services and PCS is the one-number service to be offered by PCS. A single-number system allows maximum personal mobility. Under this concept, a single directory number would be used to direct all calls to a user wherever he or she is. Cellular 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 or 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 wire-line 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 subject's 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 ser-

vices 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.

AIN¹⁹ 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.

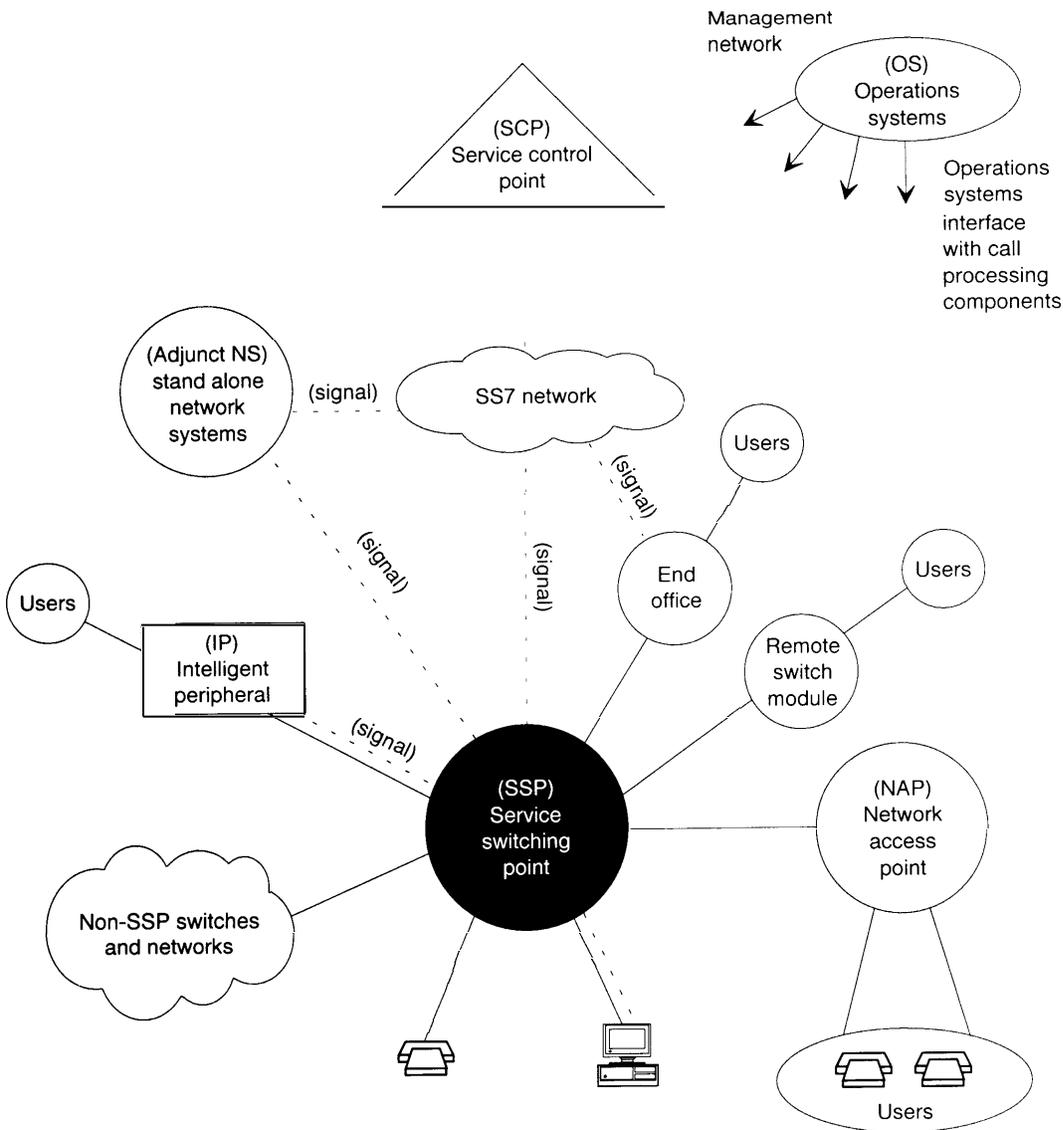
A Service Switching Point (SSP, See figure 2-8 above.), is a special kind of switch (e.g., an end office switch or a tandem switch) that contains AIN switch capabilities. A SSP can identify calls associated with AIN services. When a call is identified that requires AIN treatment, the SSP initiates a 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.

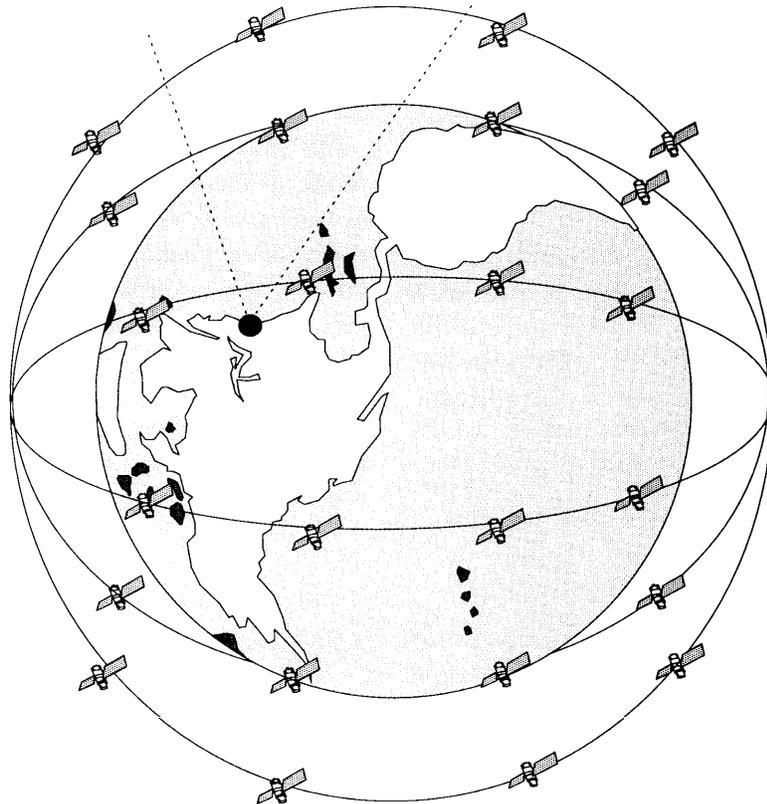
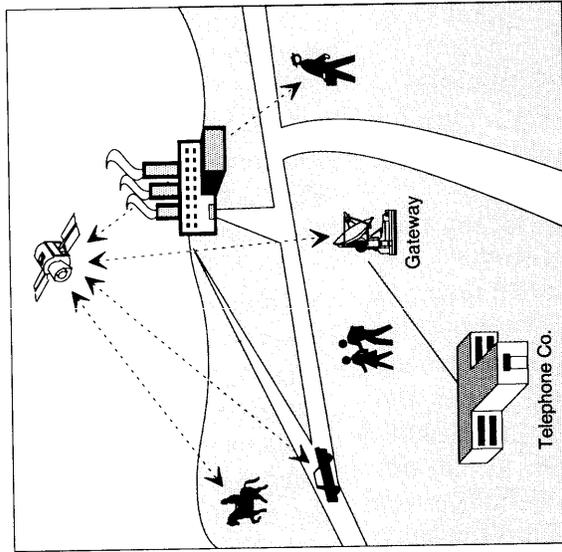
Big LEOS can provide a wide range of voice and data services, including all of the services provided by Little LEOS, plus cellular- or PCS- like telephone service. Communications can be from mobile or fixed Earth stations. These satellite-linked services are considered to be possible alternatives to 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* system²⁴ 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 (Equatorial Constellation Communications—Constellation Communications, Inc., Bell Atlantic Enterprises International, and Telecomunicacoes 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.

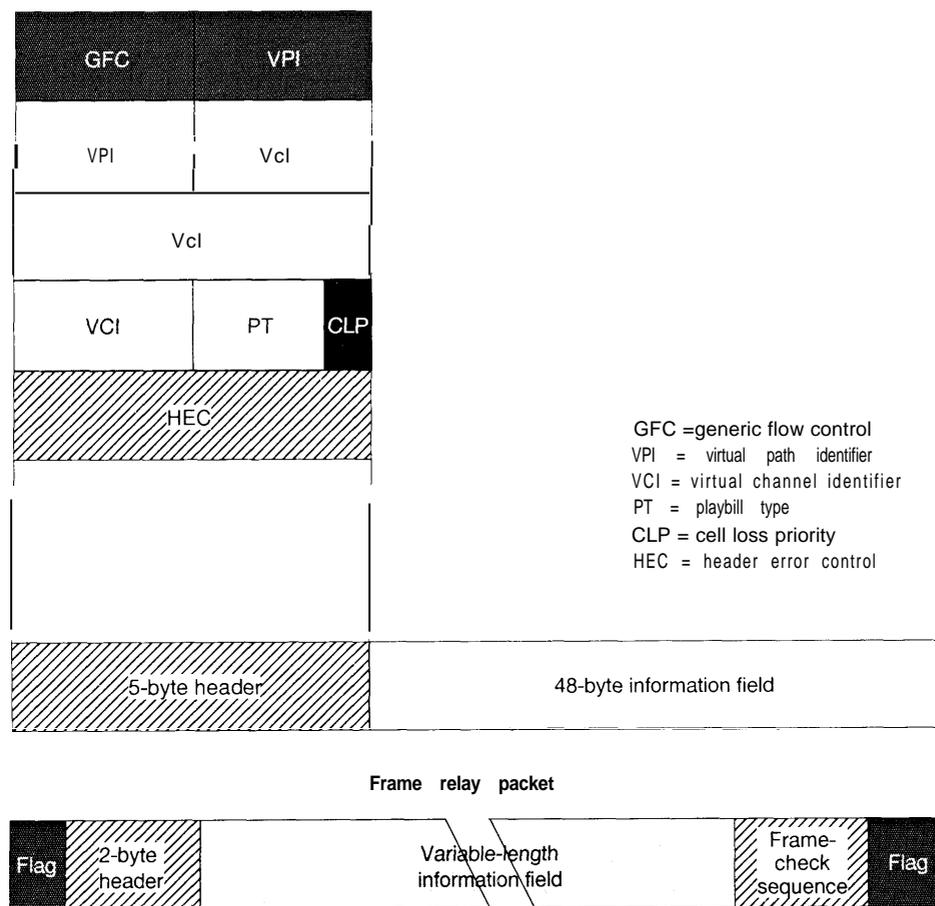
Each ATM switch is provided with a set of lookup tables (computer database), which identify an incoming cell by header address, route it through the switch to the proper output port, and overwrite the incoming address with a new one that the next switch along the route will match with an entry in its 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=virtual path identifier, VCI=virtual channel identifier; PT=playbill type, CLP=cell loss priority, 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:

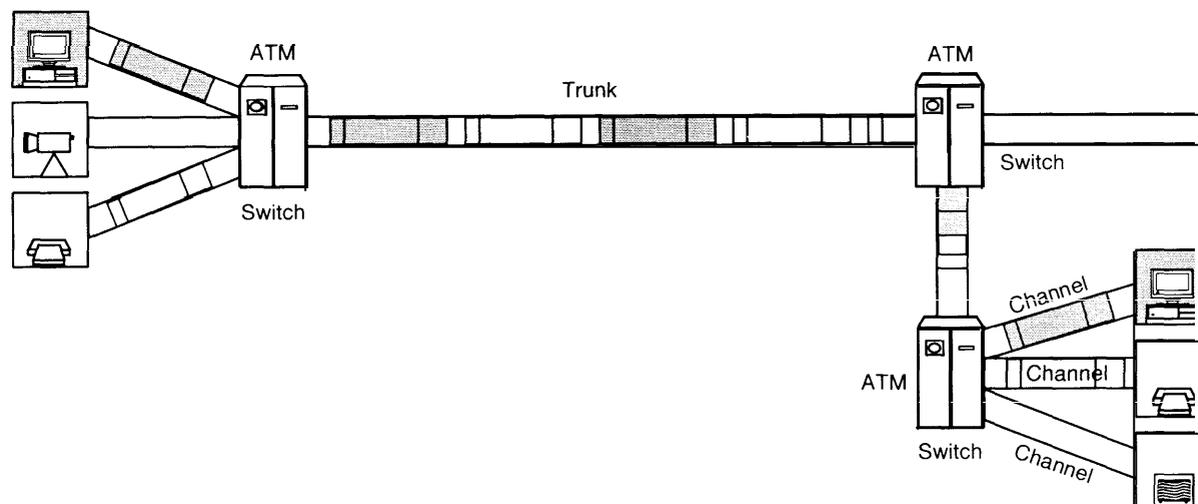
1. Virtual Path Identifier (VPI); and
2. Virtual Channel Identifier (VCI).

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 Office 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 inter-

cept 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.