TB: working doc.

Law Enforcement

REQUIREMENTS

For The Surveillance Of Electronic Communications

June 1994

Prepared by the Federal Bureau of Investigation (FBI)
in cooperation with federal, state, and local
law enforcement members of the National
Technical Investigators Association

TABLE OF CONTENTS

		Page Number
1.	INTRODUCTION	1
	1.1 Background	1
	1.2 Scope	2
	1.3 Document Organization and Maintenance	3
2.	REQUIREMENTS	5
3.	CLARIFICATIONS AND EXAMPLES	7
	3.1 Requirement 1 (Communications Access)	7
	3.1.1 Call Setup Information	8
	3.1.2 Call Content	12
	3.1.3 Mobility	14
	3.2 Requirement 2 (Real-time/Full-time Monitoring)	17
	3.3 Requirement 3 (Transmission)	17
	3.4 Requirement 4 (Transparency)	19
	3.5 Requirement 5 (Verification Information)	20
	3.6 Requirement 6 (Simultaneous Intercepts)	21
	3.7 Requirement 7 (Expeditious Access)	22
	3.8 Requirement 8 (Reliability)	23
	3.9 Requirement 9 (Quality)	23
GLOSSARY		24

LIST OF EXHIBITS

		Page Number
3-1	Information About Calls Terminating to the Intercept Subject	9
3-2	Information About the Subject's Line When the Subject Originates a Call	10
3-3	Call Redirection Scenarios	11
3-4	Wireline and Mobile Communications Examples	13
3-5	A Mobile Intercept Subject's Communications	15
3-6	Registration Information Exchange	16

1. INTRODUCTION

In July 1992, the Federal Bureau of Investigation, in cooperation with federal, state, and local law enforcement agencies, published a document entitled *Law Enforcement Requirements for the Surveillance of Electronic Communications.* The document outlined law enforcement's nine requirements for the surveillance of electronic communications. As a result of discussions between law enforcement and industry, law enforcement has prepared clarifications and examples to support the requirements contained in the July 1992 document. These clarifications and examples respond to specific questions raised by the electronic communications industry. This document states law enforcement's nine requirements and provides supporting clarifications and examples, thereby superseding the July 1992 document.

1.1 Background

The primary mission of federal, state, and local law enforcement agencies is to enforce the laws of their respective jurisdictions. Various federal and state laws authorize the interception of electronic communications for the investigation of serious crimes. This extraordinary technique is critical to law enforcement's mission. Law enforcement agencies can conduct lawfully authorized electronic surveillance when traditional investigative techniques are determined to be ineffective or too dangerous.

To conduct lawful electronic surveillance, law enforcement agencies require access to the communications associated with the subject of investigation (that is, intercept subject). In this process, law enforcement agencies rely on the cooperation and assistance of the providers of electronic communications services. A number of legal instruments permit law enforcement to collect information on or about a subject's electronic communications. These instruments include court orders (such as pen register, Title III, traps, and traces), search warrants, subpoenas, and other lawful authorizations.

Recent and continuing advances in electronic communications technology and services challenge, and at times erode, the ability of law enforcement agencies to fully implement lawful orders to intercept communications. These advances also challenge the ability of electronic communications service providers to meet their

assistance responsibilities. The law enforcement community needs the continued cooperation of electronic communications service providers to meet the challenges of conducting electronic surveillance on emerging and future technologies. Law enforcement is not seeking to slow the pace of the evolution of electronic communications. In fact, advanced communications features and services benefit law enforcement and the American public. As new technologies and services emerge, law enforcement is attempting only to ensure that capabilities exist for protecting public safety through the use of lawful interception.

1.2 Scope

This document presents the requirements of federal, state, and local law enforcement agencies to conduct lawful electronic surveillance with regard to users of electronic communications services. Its purpose is (1) to serve as a framework for continued cooperation with the electronic communications industry in the development of approaches for meeting law enforcement's electronic surveillance requirements, and (2) to preserve electronic surveillance capabilities associated with intercept authority as established by applicable federal and state laws.

The requirements are intended to set out key elements needed for the technical and operational implementation of lawful interceptions of electronic communications. Although the requirements are intended to be broad enough to address existing or future communications technologies, the clarifications and examples supporting the requirements may be specific to a current technology or service. As additional technologies emerge, new communications services and features will be introduced after the publication of this document. Consequently, the information presented in this document may not be all-inclusive. Law enforcement recognizes the need to ensure an understanding of the requirements as the electronic communications industry accommodates the requirements in the development of technologies and services. Law enforcement also understands the need to periodically clarify the information presented in this document to account for new services and features identified by service providers.

Access to the communications of an intercept subject is made available by the service provider in accordance with a lawful authorization from law enforcement. As is the case under current statute, "No cause of action shall lie in any court against

any provider of wire or electronic communications service, its officers, employees, or agents, landlord, custodian, or other specified person for providing information, facilities, or assistance in accordance with the terms of a court order or certification under this chapter."[1] Law enforcement's requirements in no way alter the provisions of existing statutes.

1.3 Document Organization and Maintenance

The remainder of this document is organized into two sections followed by a glossary. Section 2 presents law enforcement's nine requirements for the surveillance of electronic communications. These nine requirements are listed in **bold** type and are the same as those presented in *Law Enforcement Requirements for the Surveillance of Electronic Communications*, July 1992. The words used to express Requirements 1, 3, and 5 have been modified to better convey their intent based on comments received from industry. The textual modifications are as follows:

- In Requirement 1, the original text was modified to clarify that the requirement is for access to communications transmitted to and from any identifier associated with the intercept subject (not just the identifier of the intercept subject's terminal equipment). Text was also added to clearly convey that a service provider served with a lawful authorization is responsible for providing law enforcement with access to an intercept subject's communications while the subject is within service areas operated by that service provider. Access is required as long as the service provider maintains access to the intercept subject's communications. Law enforcement is not asking for an automatic, seamless, nationwide intercept capability for subjects traveling across multiple service provider boundaries. *In all circumstances, access to network features used to intercept a subject's communications is controlled by service providers and not by law enforcement agencies.*

[1] 18, U.S.C. 2511 (2)(c)(ii)

- In Requirement 3, the term "remote" and the words "away from the intercept access point and/or the intercept subject's terminal equipment" have been deleted to remove confusion regarding the intent of this requirement. The changes reinforce the intent of the requirement. Once a service provider has access to the intercepted communications, law enforcement requires delivery of the communications to a designated monitoring facility. Again, access to any intercept feature is controlled by the service provider and not by law enforcement agencies.

- In Requirement 5, the words "prior to intercept implementation and during the intercept" were moved to the end of the sentence to clarify the requirement. Requirement 5 states that information is required to verify the association of the intercepted communications with the intercept subject. This requirement also states that information on a subject's services and features is required and may be requested before intercept implementation or during the intercept.

Section 3 provides a set of supporting clarifications and examples for each requirement. A glossary containing a list of key words and phrases used in the requirements follows Section 3.

Due to the continuing evolution of electronic communications technology, this document will be reviewed periodically and updated as needed. Any comments or recommendations should be forwarded to:

Assistant Director
Information Resources Division
Federal Bureau of Investigation
JEH FBI Building
10th and Pennsylvania Avenue, N. W.
Washington, DC 20535

2. REQUIREMENTS

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

Requirement 2 Law enforcement agencies require a real-time, full-time monitoring capability for intercepts.

Requirement 3 Law enforcement agencies require service providers to transmit intercepted communications to a monitoring facility designated by the law enforcement agency.

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

Requirement 5 Law enforcement agencies require (1) information from the service provider to verify the association of the intercepted communications with the intercept subject, and (2) information on the services and features subscribed to by the intercept subject prior to and during the intercept implementation.

Requirement 6 Law enforcement agencies require service providers to make provisions for implementing a number of simultaneous intercepts. (Intercept demand will be estimated through a cooperative industry and law enforcement effort.)

Requirement 7 Law enforcement agencies require service providers to expeditiously provide access to the communications of the intercept subject.

Requirement 8 Over the intercept period, law enforcement agencies require that the reliability of the services supporting the intercept at least equals the reliability of the communication services provided to the intercept subject.

Requirement 9 Law enforcement agencies require the quality of service of the intercepted transmissions forwarded to the monitoring facility to comply with the performance standards of the service providers.

3. CLARIFICATIONS AND EXAMPLES

The nine requirements presented in Section 2 are restated in this section in **bold** type. Paragraphs containing clarifications and examples follow each requirement as a means for conveying overall intent. Law enforcement's surveillance authorities include all forms of electronic communications. However, as a result of intensive discussions with the telecommunications industry, most of the clarifications and examples in this section are in terms of telephony, but apply equally to all electronic communications service providers. The clarifications are only illustrative and are an aid for interpreting the intention of the requirement. The nine requirements in bold type fully encompass and reflect law enforcement's requirements for lawful intercepts and are not intended to be replaced or limited by the clarifications and examples provided in this section.

3.1 Requirement 1 (Communications Access)

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

The primary requirement of law enforcement agencies is for access to the electronic communications transmitted, or caused to be transmitted, to and from the intercept subject. In all circumstances, access to network features used to intercept a subject's communications is controlled by service providers and not by law enforcement agencies. The requirement for access to an intercept subject's communications by law enforcement does not imply automatic activation or deactivation of intercepts. Law enforcement agencies will continue to interface with service provider security personnel to request intercept activation and deactivation.

Under Requirement 1, access to an intercept subject's communications includes call setup information and call content. Law enforcement agencies need access to call setup information (for example, originating line/number

identification, terminating line/number identification) for all completed and attempted calls. An attempted call is a call that was initiated, but failed to establish a connection between the calling and called parties (for example, when a busy signal was received). Access to call content is required for calls placed by and to the intercept subject, including calls that have been redirected or have multiple call recipients. The obligation of service providers to provide access when custom calling features are invoked depends on whether the service provider that received the authorized intercept request maintains access to the call.

The requirement for lawful access to call content and call setup information also applies to mobile telecommunications services. Law enforcement requires access to an intercept subject's communications throughout the service areas operated by the service provider served with a lawful authorization. With the use of emerging technologies, the location of an intercept subject's access to the network may vary during a call or call attempt (for example, while roaming or when redirecting calls). Law enforcement recognizes the need to coordinate the delivery of communications with service providers before interception occurs.

3.1.1 Call Setup Information

Law enforcement agencies require access to all available call setup information for all attempted and completed calls originated by or terminating to the intercept subject. Call setup information includes, but is not limited to the following:

- Information regarding the intercept subject's line[2]
- Information regarding the calling party's line
- Dialing and signaling information generated by the intercept subject
- Directory numbers used in transferring or forwarding calls
- Notification that a call or call attempt occurred.

Line Information for Terminating Calls. Law enforcement agencies require access to call setup information for all completed and attempted calls to the intercept

[2] The term "line" is used broadly to refer to the transmission path from a subscriber terminal to the network. This transmission path may be via a wireline or wireless medium (for example, copper wire, radio link).

subject. In this case, call setup information refers to information on both the subject's and the calling party's line. Access to information about the subject's line is required for all calls terminating to the intercept subject. Access to information about the calling party's line is required when it is delivered to the service provider supporting the called intercept subject's communications. The type of line information available for both parties depends on the communications services in use by the calling party and the intercept subject. Exhibit 3-1 lists a number of examples.

Exhibit 3-1
Information About Calls Terminating to the Intercept Subject

CALLING PARTY'S LINE INFORMATION	SERVICE TYPE	INTERCEPT SUBJECT'S LINE INFORMATION
• Directory Number (DN)	Plain Old Telephone Service (POTS)	• Directory Number (DN)
• Associated Directory Number • Line Equipment Identifier • Call Type/Bearer Capability • Service Profile Identifier (SPID)	Integrated Services Digital Network (ISDN)	• Associated Directory Number • Line Equipment Identifier • Call Type/Bearer Capability • Service Profile Identifier (SPID)
• Numbers used by the service provider switch to identify the PBX and the caller behind the PBX - Directory Number of the PBX - Station identifier of the calling party (if available)	Private Branch Exchange (PBX)	• Numbers used by the service provider switch to identify the PBX and the caller behind the PBX - Directory Number of the PBX - Station identifier of the called party (if available)
• Directory Number	Coin	• Directory Number
• Electronic Serial Number (ESN) • Mobile Identification Number (MIN)	Cellular	• Electronic Serial Number (ESN) • Mobile Identification Number (MIN)
• Personal Number/Directory Number • Terminal Equipment Identifier	Personal Communications Service (PCS)	• Personal Number/Directory Number • Terminal Equipment Identifier
• Directory Number • Other available items, for example, Automatic Numbering Identification (ANI)	Other Special and Proprietary Customer Premises Equipment (CPE) Interfaces (Non-POTS or Non-ISDN Signaling)	• Directory Number • Other available items, for example, Automatic Numbering Identification (ANI)

Line Information for Originating Calls. When the intercept subject originates a call, law enforcement requires access to information about the communications

line used by the subject. The information available to describe a subject's line varies based on the type of communications service used by the intercept subject. Types of line identifiers include directory numbers (DN), mobile identification numbers (MIN), and personal numbers. Exhibit 3-2 presents several examples of information needed about a subject's line and required by law enforcement agencies when the intercept subject originates a call.

Exhibit 3-2
Information About the Subject's Line When the Subject Originates Calls

SERVICE TYPE	LINE INFORMATION
Plain Old Telephone Service (POTS)	• Directory Number (DN)
Integrated Services Digital Network (ISDN)	• Directory Number Associated With the Call • Line Equipment Identifier • Call Type/Bearer Capability • Service Profile Identifier (SPID)
Private Branch Exchange (PBX)	• Numbers used by the service provider switch to identify the PBX and the caller behind the PBX: - Directory Number of the PBX - Originating station identifier
Coin	• Directory Number
Cellular	• Electronic Serial Number (ESN) • Mobile Identification Number (MIN)
Personal Communications Service (PCS)	• Personal Number/Directory Number • Terminal Equipment Identifier
Other Special and Proprietary Customer Premises Equipment (CPE) Interfaces (Non-POTS or Non-ISDN Signaling)	• Directory Number • Other available items, for example, Automatic Numbering Identification (ANI)

Dialing and Signaling Information. In addition to the subject's line information, law enforcement agencies require access to the dialing and signaling information generated by the subject for all calls originated by the intercept subject. Examples of dialing and signaling information include the following:

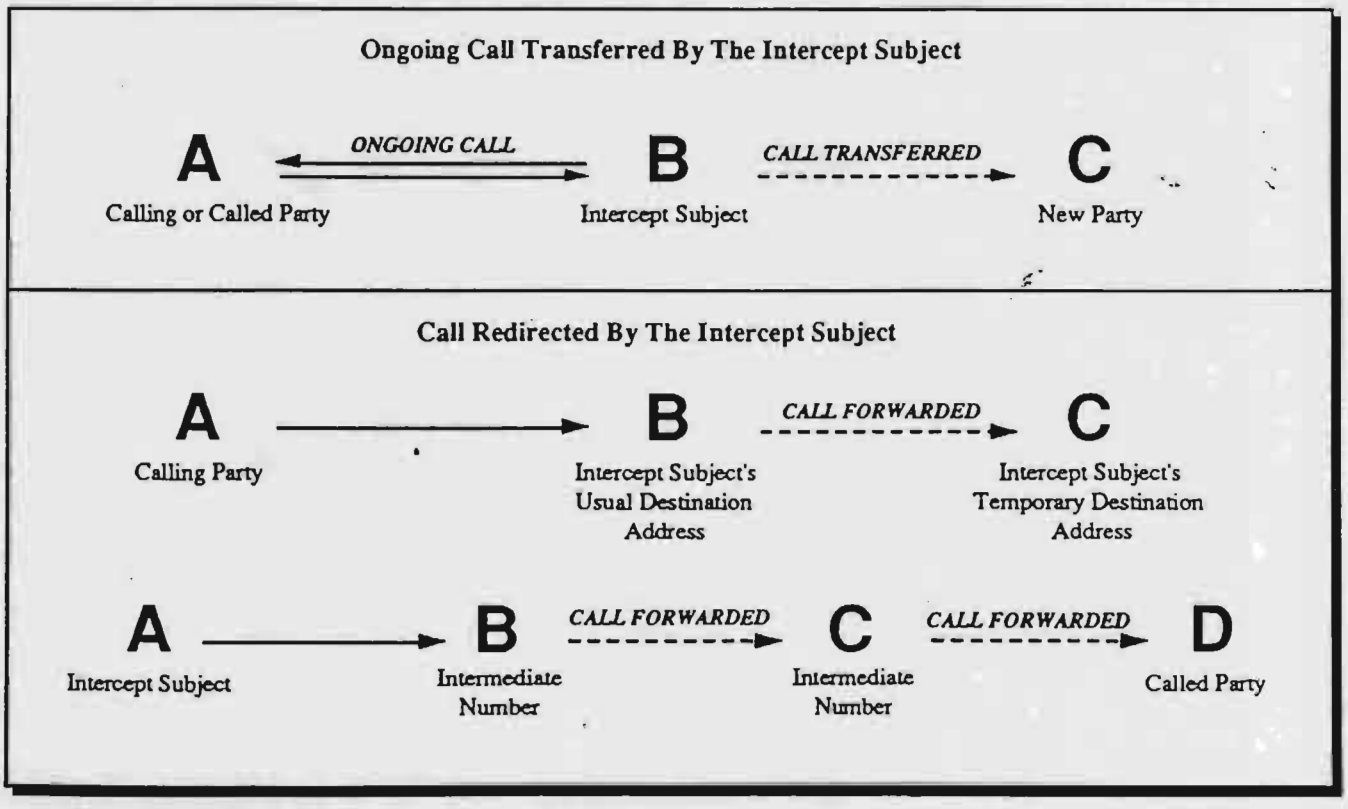
- All digits dialed by the subject and any signaling information used to establish or direct call flow

- Subsequent dialing information generated by the subject after cut-through

- The terminating number of the destination derived by the originating switch based on its interpretation of the subject's dialed digits or other call direction commands.

Redirection Numbers. Access to call setup information also includes redirection numbers when calls are forwarded or transferred using custom calling features. Law enforcement requires access to the forwarded-to number when the intercept subject transfers or forwards calls to another number. For a call terminating to the intercept subject, law enforcement agencies require access to any available redirection numbers when multiple forwards or transfers are involved in the call attempt. As an example, a call initiated by a calling party may be forwarded or transferred several times before reaching the intercept subject. Law enforcement requires the number of the calling party that originated the call, as well as any available intermediate numbers used to redirect the call. Exhibit 3-3 illustrates several call redirection scenarios.

Exhibit 3-3
Call Redirection Scenarios*



* A, B, C, and D may represent the same or different switches

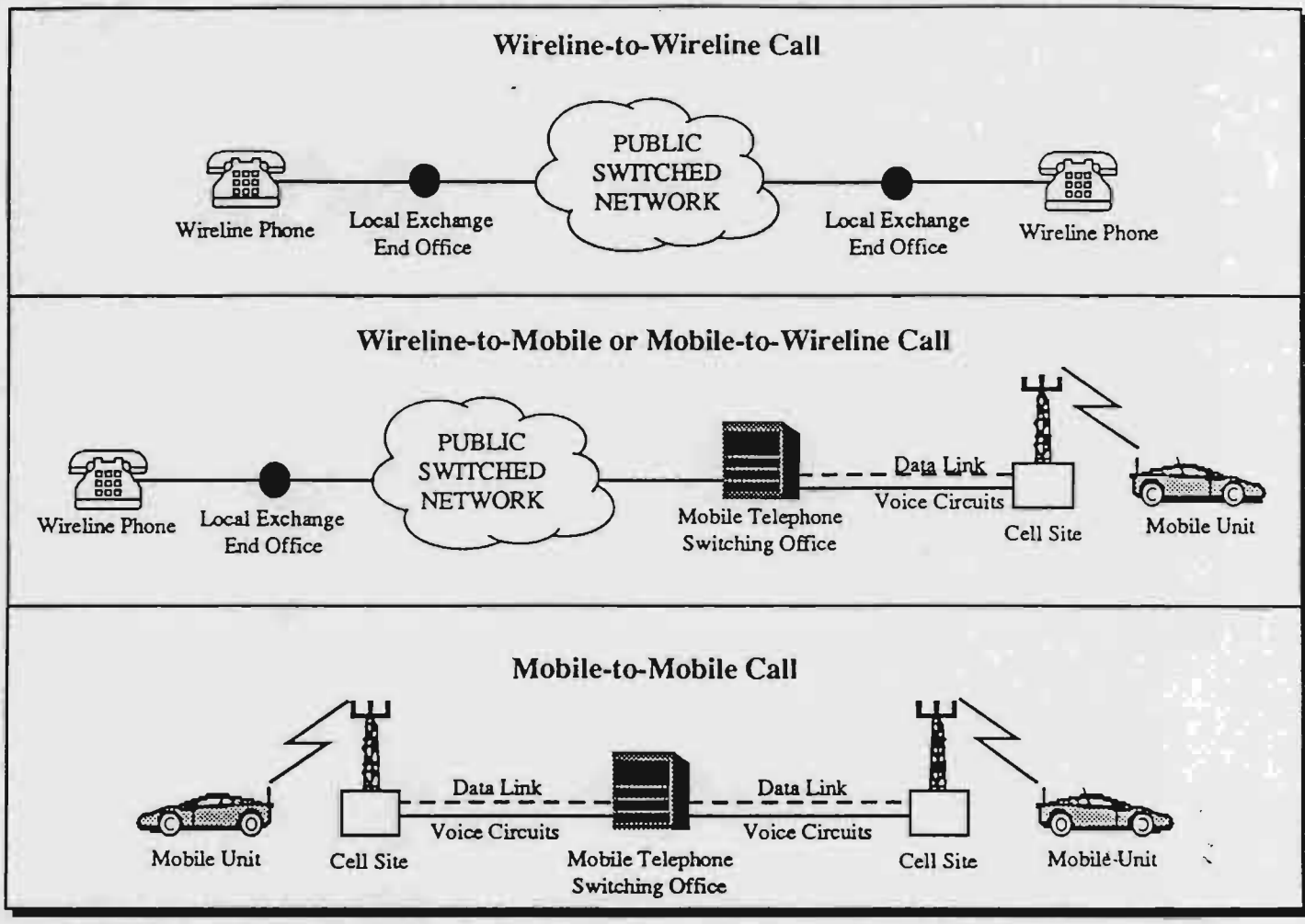
Call Attempt Alerts. Law enforcement agencies require notification of all call attempts placed to or by the intercept subject. For example, in the case of a wireline intercept on a local loop, law enforcement generates a time stamp after detecting the local exchange carrier's (LEC) signaling for on-hook, ringing, and off-hook. However, local exchange carrier signaling protocols may change with emerging technologies. In future implementations, out-of-band signaling using signaling transfer points (STP) may replace in-band protocols currently used by law enforcement to detect call activity. Therefore, law enforcement agencies require some form of notification to provide a trigger for monitoring equipment.

3.1.2 Call Content

Law enforcement agencies require access to call content for all calls originating from and terminating to the intercept subject's fixed or mobile number, terminal equipment, or other identifier. Access to call content is required regardless of the type of communications used in the call including cases when the communications between the intercept subject and other parties are sent and received over separate channels. The communications between the intercept subject and other parties may take place using wireline systems, wireless (mobile) systems, or a combination.

Service Arrangements. In a wireline-to-wireline call, both the calling and called parties use traditional wireline services. Examples of wireline services include coin, Plain Old Telephone Service (POTS), and Integrated Services Digital Network (ISDN). In a wireline-to-mobile or mobile-to-wireline call, one party uses a mobile communications service while the second party uses a wireline service. With mobile communications services, the service subscriber is able to communicate as he or she moves within a given region or area. Cellular and Personal Communications Service (PCS) are examples of mobile services. When both parties use a mobile service, the call is referred to as mobile to mobile. Exhibit 3-4 illustrates these types of call scenarios.

Exhibit 3-4
Wireline and Mobile Communications Examples



In each of the scenarios presented in Exhibit 3-4, the call is switched by a specific entity before terminating to or after being originated by the intercept subject. Law enforcement agencies require access to call content regardless of the entities used to switch the calls. For example, in a mobile-to-mobile or wireline-to-mobile call, the call may be switched at a cell site, at a Mobile Telephone Switching Office (MTSO), or at a Personal Communications Switching Center (PCSC).

Custom Calling Features. Access to call content includes calls that have been redirected or have multiple call recipients. The obligation of service providers to provide access when custom calling features are invoked depends on whether the service provider that received the authorized intercept request maintains access to

the call. When custom calling features are invoked, the service provider that received the authorized intercept request is required only to provide access to call content as long as the service provider maintains access to the communications. When an intercept subject uses a redirection feature that causes the loss of call access by the service provider, law enforcement requires notification of the identity of the new service provider now supporting the subject's communications. If the new service provider's identity is unavailable, law enforcement requires any information that will permit law enforcement agencies to determine the new service provider's identity. *In all cases, law enforcement agencies will coordinate delivery of communications in advance.*

3.1.3 Mobility

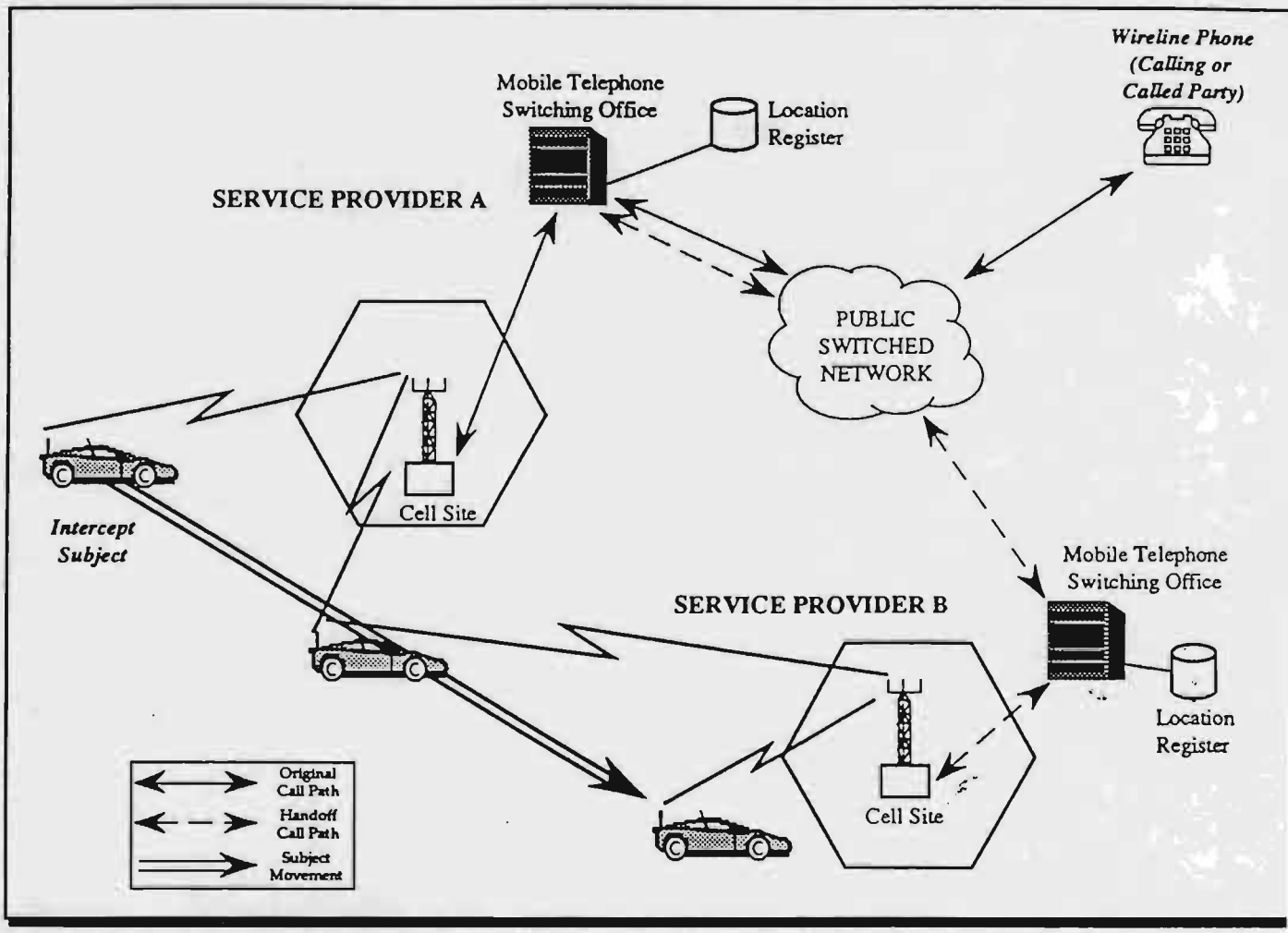
The requirement for lawful access to call content and call setup information applies equally to mobile telecommunications services. With mobile telecommunications services, a subscriber may move freely within predefined areas and communicate using portable units, terminals, or personal numbers. Law enforcement requires access to an intercept subject's communications throughout the service areas operated by the service provider that has been served with a lawful authorization to intercept. When an intercept subject travels into another service provider's area, law enforcement requires access to ongoing calls only if the service provider maintains access to the subject's communications. When access to the subject's call is not maintained, law enforcement requires the identity of the visited service provider or information that will permit agencies to determine the visited service provider's identity.

The following clarifications and examples focus on cellular communications, which is an existing and well understood technology. However, the requirements apply equally to other mobile communications services.

Handoffs. Law enforcement agencies require continuous access to all ongoing calls regardless of any handoffs that may occur, as long as the service provider retains access to the call. This includes cases where the intercept subject moves within a service provider's system or between service provider systems. Exhibit 3-5 illustrates the case when an intercept subject, using a cellular service, travels into another service provider's area during an active call. In this illustration, the Mobile

Telephone Switching Office serving the end user maintains access to the call and continues to provide law enforcement with access to the intercept subject's communications.

Exhibit 3-5
A Mobile Intercept Subject's Communications

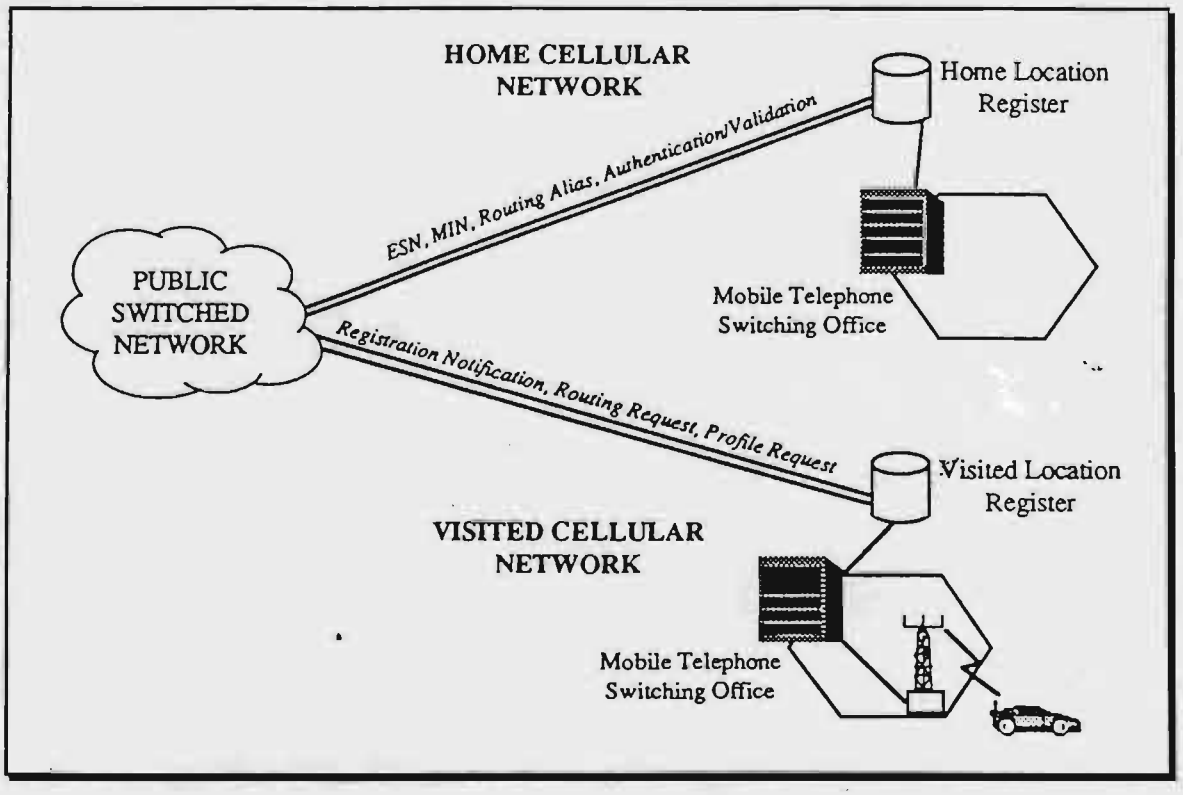


Roaming. The access requirement applies when the intercept subject uses roaming features. This requirement assumes that service providers supporting the subject's communications have received the appropriate lawful authorization from law enforcement and that delivery of the communications has been coordinated. Law enforcement is not asking for an automatic, seamless, nationwide intercept capability for subjects traveling across multiple service provider boundaries. A service provider's network may encompass local, regional, or interstate areas

depending on the scope of service coverage offered by the service provider. However, when a service provider offers a nationwide service and lawful authorizations permit interception, law enforcement agencies require access to communications for an intercept subject roaming within that service provider's network.

Registration Information. Law enforcement agencies require access to information regarding the identity of service providers requesting visit registration authorization for an intercept subject. For cellular services, Exhibit 3-6 depicts the case when an intercept subject travels into a new service provider's area and requests service.

Exhibit 3-6
Registration Information Exchange



The exhibit illustrates that during registration, information is exchanged between the original service provider's location register and the visited location register. The original service provider is under an existing lawful authorization to provide access to the intercept subject's communications. In this example, law

enforcement requires that the original service provider notify law enforcement of the new service provider's identity, or provide any other information that permits law enforcement agencies to determine the identity of the visited service provider.

Service Site Information. In certain situations and with appropriate lawful authorizations, law enforcement agencies may request the most accurate information available from the service provider's network elements regarding the site from which services are being provided to the intercept subject. For example, in a cellular system, service site information may include the cell site serving the intercept subject or the identity of the service provider supporting communications after a handoff.

3.2 Requirement 2 (Real-time, Full-time Monitoring)

Law enforcement agencies require a real-time, full-time monitoring capability for intercepts.

Real-time/Full-time Access. Law enforcement agencies require real-time access to an intercept subject's communications content and call setup information. The term "real-time" in Requirement 2 refers to monitoring that occurs as the intercepted communications take place, rather than the monitoring of a recording of the communications. In actuality, there is a small transmission delay from the moment intercepted communications occur to the moment the signals reach the monitoring equipment. Real-time monitoring of data communications may occur at any time between the sending of a data transmission by the originating terminal equipment and the receiving of the data transmission by the destination terminal equipment. Full-time monitoring refers to the ability to access and monitor all service activity associated with the intercept subject on a 24 hour-per-day basis.

3.3 Requirement 3 (Transmission)

Law enforcement agencies require service providers to transmit intercepted communications to a monitoring facility designated by the law enforcement agency.

Transmission of Intercepted Communications. Law enforcement agencies require the transmission of the intercept subject's call content and call setup

information to a designated law enforcement monitoring facility. Access to intercept features is controlled by service providers. Law enforcement agencies will work with service providers in advance to arrange for delivery of intercepted communications to a monitoring location. Guidelines for the transmission of intercepted communications are:

- If call setup information and call content are separated, law enforcement agencies require service providers to ensure accurate association of call setup information with call content.

- Law enforcement agencies require service providers to be able to transmit the intercepted communications to a monitoring location without altering the call content or meaning (exclusive of any signal formats required for delivery to law enforcement).

- Law enforcement agencies require that the facilities and format for transmitting the intercepted communications to the monitoring location be standard or generally available (for example, leased line, switched connection, analog voice). The formats will be jointly agreed upon by law enforcement and service providers.

- If the service provider controls and/or provides coding, compression, encryption, or any other security technique on the intercepted communications, law enforcement agencies require the service provider to decode, decompress, or decrypt the intercepted communications or provide capabilities for decoding, decompressing, or decrypting the communications.

- Law enforcement agencies require that service providers use a minimum number of transmission facilities to deliver the intercepted communications to the monitoring facility (for example, today most intercepts for cellular communications in service areas with multiple MTSOs require a connection from each MTSO to the monitoring location for one intercept subject).

As new technologies and services are developed, law enforcement agencies require that service providers have the ability to upgrade the delivery mechanism over time, allowing for phased changes in law enforcement collection systems.

3.4 Requirement 4 (Transparency)

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

Transparency of Interception. The intercept must remain transparent to all parties except for the monitoring agency and the electronic communications industry personnel involved in implementing the intercept. Law enforcement agencies require that the intercept remain transparent to the intercept subject, to all parties called by or calling the intercept subject, and to any other service subscribers not directly involved in communications with the intercept subject. At a minimum, the transparency of an intercept may be measured by the following attributes:

- Indications that an intercept is underway should not be discernible to the subject or other parties.

- If the implementation of an intercept occurs during an ongoing call, the intercept should not disrupt or interrupt the ongoing call (that is, no interruption or alteration of communications on active channels).

- If the implementation of an intercept causes changes in the operation of services and features, such changes should not be perceptible to the subject or other parties.

- If any noise is introduced by the implementation of an intercept, such noise should not be perceptible to the subject or other parties.

Safeguards for Intercept Access and Transparency. Service providers are not expected to ensure transparency beyond the capabilities of their own equipment.

There may be cases where the subject possesses sophisticated equipment to detect intercepts. To meet transparency requirements, the services provided to the intercept subject or any other subscriber should continue to comply with industry standards for transmission characteristics.

Law enforcement agencies also require that the service provider's operating procedures contain safeguards to preclude unauthorized or improper use of intercepts and to prevent a compromise of transparency. Example safeguards include:

- Restrictions on access to information about intercepts
- Security mechanisms for activating and deactivating intercepts (for example, passwords)
- Physical security to limit access to systems supporting intercepts
- Procedures to prevent subjects from being notified of service changes caused by the implementation of intercepts
- Restriction of knowledge of intercepts to authorized service provider personnel (that is, personnel with a "need-to-know").

Service providers must immediately notify the appropriate law enforcement agency upon learning that intercept transparency was or may have been compromised.

3.5 Requirement 5 (Verification Information)

Law enforcement agencies require (1) information from the service provider to verify the association of the intercepted communications with the intercept subject, and (2) information on the services and features subscribed to by the intercept subject prior to intercept implementation and during the intercept.

Information Associating Communications With the Intercept Subject. Based on lawful inquiry, law enforcement agencies require information to verify the association of the intercepted communications with the network identifier (for

example, directory number), terminal equipment identifier, and/or personal number of the intercept subject designated in the lawful authorization. Specifically, court authorities require law enforcement agencies to verify that the communications facility or service being intercepted corresponds to the subject or subjects identified in the lawful authorization. To accomplish the verification, law enforcement needs information, such as billing and caller identification-related information, from service providers. Service providers are not expected to provide information about the type of communications (for example, facsimile, electronic mail) or the customer premises equipment used by the intercept subject.

Service Profile Information. Law enforcement agencies also require that a subject's service profile information be made available upon a lawful inquiry. Service profile information may be requested before or during interception. Law enforcement agencies require notification from service providers of changes made to the intercept subject's service profile during an ongoing intercept regardless of how the changes are initiated. For example, a service profile change may be driven by a service order or directly initiated by the intercept subject.

3.6 Requirement 6 (Simultaneous Intercepts)

> **Law enforcement agencies require service providers to make provisions for implementing a number of simultaneous intercepts. (Intercept demand will be estimated through a cooperative industry and law enforcement effort.)**

Multiple, Simultaneous Intercepts. Law enforcement agencies need to be able to perform multiple, simultaneous intercepts within a given service provider's system, central office, area, etc. Law enforcement agencies and industry will need to work together to determine capacity ranges for use in developing intercept capabilities for a changing telecommunications environment. Law enforcement agencies require a service provider to support all requested lawfully authorized intercepts within its service area. As a result, law enforcement agencies require service providers to have reserve intercept capacities available to meet unexpected intercept demands that exceed projections. Law enforcement and industry should work together to achieve a "no held order" operating environment (that is, an environment where all intercept orders are fulfilled by service providers).

Interception of Multiple Calls and by Multiple Agencies. Law enforcement agencies need the ability to access and monitor all simultaneous calls originated or received by the intercept subject. In accordance with Requirement 4, multiple law enforcement agencies require the ability to monitor the same intercept subject while maintaining transparency.

3.7 Requirement 7 (Expeditious Access)

Law enforcement agencies require service providers to expeditiously provide access to the communications of the intercept subject.

Access Activation/Deactivation. Law enforcement agencies require each service provider to have defined or standardized procedures for activating and deactivating intercepts, and to provide access to the intercept subject's communications within 24 hours or less upon receipt of a lawful intercept request. Law enforcement agencies may also require expeditious access to appropriate technical resources or points of contact for assistance in activating the intercept or acquiring necessary service information (for example, service site information or service profile information).

Access Under Special Conditions. When special inside or outside plant construction is required to implement the intercept (for example, the construction of a leased line), law enforcement agencies require access to the intercept subject's communications within 5 business days or a period determined feasible by the service provider and law enforcement. In "emergency situations," law enforcement agencies require access to the intercept subject's communications within a few hours, and access to technical resources for assistance with the intercept. Law enforcement may elect to defer some requirements in certain exigent circumstances, thereby enabling a service provider to comply with an order to meet urgent investigative needs. Emergency situations are determined by law enforcement and apply to time-critical investigations, such as cases where rapid response is required to eliminate threats to life, property, or national security. Law enforcement will provide service providers with as much prior notification as possible. "Emergency" situations relate to electronic surveillance conducted pursuant to United States Code.[3]

---

[3] 18, U.S.C. 2518 (7); 18, U.S.C. 2518 (11) (b); 18, U.S.C. 3125 (a); 50, U.S.C. 1805 (e)

3.8 Requirement 8 (Reliability)

During the intercept period, law enforcement agencies require that the reliability of the services supporting the intercept at least equals the reliability of the communication services provided to the intercept subject.

Reliability of Intercept. Law enforcement agencies require that the reliability of the service supporting the intercept be at least equal to the reliability of the subject's service. Reliability refers to the probability that a system or product will perform in a satisfactory manner for a given period of time when used under specified operating conditions. Law enforcement agencies also require that service providers have the ability to detect and resolve problems with (1) the interception of call setup information and call content, and with (2) the transmission of the intercepted communications to the designated monitoring facility. Finally, law enforcement agencies require that service providers have plans for ensuring that system upgrades, software upgrades, and other network management procedures do not disrupt or terminate ongoing intercepts.

3.9 Requirement 9 (Quality)

Law enforcement agencies require the quality of service of the intercepted transmissions forwarded to the monitoring facility to comply with the performance standards of the service providers.

Quality of Intercept. Law enforcement agencies require that the quality of the service supporting the intercept be at least equal to the quality of the subject's service. Quality of service in regard to the intercept refers to the quality specification of the communications channel or system used to transmit the intercepted communications. For example, quality of service may be measured based on signal-to noise ratio, bit error rate, or any other parameter for transmission quality.

GLOSSARY

Access	The technical capability to interface with a communications facility, such as a communications line or switch, so that law enforcement can monitor and receive call setup information and call content.
Call	Any wire or electronic signaling information generated by a human or a computer acting as an agent for a human to set up a physical or virtual connection to transmit information to another or multiple users (humans and/or computer processes).
Call Content	The same as "contents," as defined in 18, U.S.C. 2510 (8) and with respect to any electronic communication, includes any information concerning the substance, purport, or meaning of that communication.
Call Setup Information	When used with respect to any electronic communication, the information generated during the establishment of communications or transmission of a protocol data unit, such as a datagram, that identifies the origin and destination of the call. For voice communications, this information is typically the electronic pulses, audio tones, or signaling messages that identify the numbers dialed or otherwise transmitted, or caused to be transmitted, by the intercept subject. It also includes incoming pulses, tones, or messages that identify the number of the originating instrument, device, or user. For data services, this information is typically the source (calling) address and destination (called) address contained in fields of the data unit, such as in the header of a frame or packet.

Electronic Communications	The same as defined in Section 2510 (12) of 18, U.S.C., any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic photo-electric, or photo-optical system, etc. As used herein, the term includes "wire communications," as defined in 18, U.S.C. 2510 (1).
Electronic Surveillance	The statutory-based process and the associated technical capability and activities of law enforcement agencies related to the interception and monitoring of electronic communications.
Inside Plant Construction	With respect to wire and cable, any modification to the cable plant extending inward beyond the cable vault (for example, central office equipment, local area network management center), including the protectors and associated hardware. With respect to wireless networks, all fixed ground communications equipment that is permanently located inside buildings (for example, the equipment within the Mobile Telephone Switching Office of a cellular provider).
Intercept Subject	Person or persons identified in the lawful authorization and whose incoming and outgoing communications are to be intercepted and monitored.
Law Enforcement	Federal, state, and local law enforcement agencies.
Outside Plant Construction	Any modification to the physical plant, such as cables, poles, ducts, conduits, wire, fiber, repeaters, load coils, and other equipment located between central offices and other switching entities, or between the central office/switching entity and the customer.

Roaming The ability of subscribers of mobile telecommunications services to place and receive calls when they are located outside their designated home serving area.

Service Provider Any public, quasi-public, or private supplier of electronic communications services providing users the ability to send or receive electronic communications (for example, local and long distance carriers, competitive access providers, public data service providers, and cellular service providers).

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

Transparency The circumstances wherein the parties to a communication and unauthorized individuals (that is, individuals who are not involved in implementing and maintaining the intercept) are unaware of ongoing electronic surveillance. For example, when applied to telephone communications, transparency refers to the interception of communications in such a way that the user is unaware of the intercept, and that does not affect the way the telephone functions are used.

Verification The process whereby law enforcement can adequately demonstrate to a judge or jury that the number or other identifier (for example, telephone number, electronic mail address) targeted for interception corresponds to the person or persons whose communications are being intercepted. Typically, law enforcement verifies the identity of the subscriber whose facility or service is being intercepted.