TB working copy

Law Enforcement

REQUIREMENTS

For The Surveillance
Of Electronic Communications

June 19, 1992<

1. INTRODUCTION

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 conferred in Federal and State law.

1.1 Background

The primary mission of Federal, State, and local law enforcement agencies is to enforce the laws of their respective jurisdictions. These laws relate to both criminal and national security/foreign counterintelligence investigations. Hereafter, the discussion is limited to criminal investigations. By statute, only when traditional investigative techniques are determined to be unsuccessful or too dangerous can law enforcement conduct court-ordered or otherwise authorized electronic surveillance. This extraordinary technique is critical to law enforcement's mission.

To conduct lawful electronic surveillance, law enforcement needs access to the communications associated with the subjects of investigation. In this process, law enforcement needs the cooperation and assistance of the providers of electronic communications services. It is imperative that industry cooperation includes accommodation of law enforcement's intercept requirements in the development and introduction of new technology and services.

Law enforcement typically performs two types of electronic intercepts: (1) "call setup information only" and (2) "call setup information plus call content." The purpose of a call setup information only intercept is to collect information about the origin and destination of

calls placed by and to intercept subjects. A call setup information plus call content intercept involves the collection of call setup information and the real-time monitoring of the communications to and from the intercept subjects.

Recent and continuing advances in electronic communications technology and services challenge, and at times erode, the ability of law enforcement to fully implement lawful orders to intercept communications. Trends in wireline and wireless communications technologies are leading to an environment where subscribers will be offered ubiquitous, uninterrupted communications capability as they move freely from service area to service area, identified by a single personal telecommunications number, data network address, or similar identifier. Law enforcement is seeking the continued cooperation of providers of electronic communications services to meet the challenges posed to electronic surveillance by emerging and future technologies. Law enforcement does not seek to impede the evolution of electronic communications, rather it is trying to preserve intercept capabilities.

1.2 Scope

This document presents the requirements of law enforcement to effectively and fully conduct electronic surveillance. The requirements defined in this document were initially identified by a working group composed of representatives of Federal, State, and local law enforcement agencies. This document does not address approaches to meeting the requirements.

The requirements are not specific to any existing or future communications technology, equipment, or service. Law enforcement views this document as a basis for further refinement of requirements by law enforcement and the specification of technical solutions by industry.

1.3 Document Organization and Maintenance

The remainder of this document is organized into three sections. Section 2 defines words and phrases used in the requirements section. Section 3 states and discusses law enforcement's electronic surveillance requirements. A list of references is included in Section 4.

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
Technical Services Division
Federal Bureau of Investigation
JEH FBI Building, Room 7159
10th and Pennsylvania Avenue, N.W.
Washington, D.C. 20535.

2. DEFINITION OF TERMS

Access — The technical capability to interface with a communications facility, such as a communications line or switch, so that law enforcement can acquire and monitor 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 Title 18, United States Code (U.S.C.) 2510 (8), 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.

Call Setup Information Only Intercept	One of two types of law enforcement intercepts. An intercept where call setup information is collected. Pen register and trap-and-trace intercepts are examples of call setup information only intercepts.
Call Setup Information Plus Call Content Intercept	One of two types of law enforcement intercepts. An intercept where law enforcement is authorized to acquire both call setup information and the call content of the intercept subjects' communications.
Called Party	The designated party or parties receiving the call. The humans and/or computer processes requested by the calling party.
Calling Party	The humans and/or computer processes originating the call.
Communications	See Electronic Communications.
Communications Facility	The aggregate of equipment, such as telephones, computers, facsimile equipment, cables, and switches, used for various modes of transmission (e.g., digital data, audio signals, video signals).
Comprehensive	As used in association with the acquisition of call setup information, the exhaustive, complete, and thorough acquisition of any information generated during the establishment of communications that identifies the origin and destination of the call.
Continuous	As used in association with call setup information plus call content intercepts, the constant, uninterrupted access to incoming and outgoing communications.

Electronic Communications	The same as defined in Section 2510 (12) of Title 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, electro-magnetic, photoelectronic, or photooptical system, etc. As used herein, the term includes "wire communications" as defined in Title 18, U.S.C. 2510 (1).
Electronic Surveillance	As used here, the statutorily-based process and the associated technical capability and activities of law enforcement agencies related to the interception and monitoring of electronic communications.
Emergency Situations	As determined by law enforcement, an emergency situation applies to time critical investigations, such as cases where rapid response is required to eliminate threats to life, property, or national security. Typically, such a situation relates to "emergency" electronic surveillance conducted pursuant to Title 18, U.S.C. 2518 (7).
Full-time Monitoring	Continuous monitoring, 24 hours a day.
Inside Plant Construction	With respect to wire and cable, any modification to the cable plant extending inward beyond the cable vault (e.g., 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 (e.g., the equipment within the Mobile Telephone Switching Office of a cellular provider).

Intercept Access Point	The physical location within the service provider's telecommunications facilities where access to the intercepted communications or call setup information is provided. The intercept access point is not necessarily a single, fixed point and is usually not where communications are monitored (i.e., not at a law enforcement monitoring facility).
Intercept Subjects	Person or persons whose communications are to be intercepted. Intercept subjects may include multiple parties on both the incoming and outgoing sides of the communications.
Law Enforcement	Federal, State, and local law enforcement agencies.
Network Management	A set of procedures, software, equipment, and operations designed to keep an electronic communications network operating near maximum efficiency. Network management can be described in five functional areas: configuration management, fault location and repair management, security management, performance management, and administration.
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 or other switching entities, or between the central office/switching entity and the customer.
Quality of Service	The quality specification of a communications channel, system, virtual channel, computer communications session, datagram, etc. Quality of service may be measured, for example, in terms of signal-to-noise ratio, bit error rate, message throughput rate, or call blocking probability.

Real-time Monitoring	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 anytime between the sending of a data transmission by the originating terminal equipment and the receiving of the data transmission by the destination terminal equipment.
Reliability	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.
Remote Law Enforcement Monitoring Facility	A law enforcement monitoring facility that is located away from the intercept access point and/or the intercept subjects' terminal equipment.
Service Provider	Any public, quasi-public, or private supplier of electronic communications services providing users thereof the ability to send or receive electronic communications (e.g., local and long distance carriers, alternate access providers, public data service providers, cellular service providers, private branch exchange operators).
Subscriber	An individual or entity that has contracted with a service provider for electronic communications services.

Terminal Equipment	Any device, which is located at a point where information can enter or leave a communications network or system, capable of sending or receiving information over a communications channel (e.g., telephone set, facsimile machine, data terminal).
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, electro-magnetic, photoelectronic, or photooptical system.
Transparency	The circumstances wherein the parties to a communication and unauthorized individuals (i.e., individuals who are not involved in implementing and maintaining the intercept) are unaware of ongoing electronic surveillance. 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 interception, and it does not affect the way the telephone functions or is used.
Verification	The process whereby law enforcement can adequately demonstrate to a judge or jury that the number or other identifier (e.g., telephone number, electronic mail address) targeted for interception corresponds to the person or persons whose communications are being intercepted. Typically, law enforcement verifies the identity of the subscriber whose facility or service is being intercepted.

3. REQUIREMENTS

This section presents law enforcement's electronic surveillance requirements. The requirements apply regardless of:

- The identity or type of provider of electronic communications services.
- The types of services, systems, and features offered or employed by the service providers or used by the intercept subjects.
- The existing or future technologies implemented in electronic communications systems and services.
- The geographic location of intercept subjects' terminal equipment.
- The number of simultaneous intercepts requiring the assistance of a provider of electronic communications services.

All of the requirements are labeled (R) and presented in **bold** type in the document. Explanations and examples follow each requirement. Terms that are defined in Section 2 appear in *italics* the first time they are used in the requirements and supporting discussion.

(R)-1 *Law enforcement* requires *access* to the *electronic communications* transmitted, or caused to be transmitted, to and from the number or other identifier of the terminal equipment of the *intercept subjects*, as well as the *call setup information* generated necessary to identify the *calling and called parties*.

- For *call setup information only intercepts*, law enforcement requires *comprehensive* collection of call setup information, which includes information identifying the origin and destination of the *communications*, regardless of the location of the identified terminal equipment used by the intercept subjects.

- For *call setup information plus call content intercepts*, law enforcement requires comprehensive collection of call setup information and *continuous* access to the incoming and outgoing communications associated with the number or other identifier of the intercept subjects and/or their terminal equipment.

- For call setup plus call content intercepts, law enforcement requires access to *call content*, regardless of the type(s) of electronic communications transmitted individually or concurrently (e.g., voice and data concurrently transmitted via Integrated Services Digital Network [ISDN]).

Access to electronic communications and related call setup information is supplied by a *service provider* when the *calls* originate and pass through an *intercept access point* within the service provider's own system. However, in some cases today, the intercept subjects are using service provider equipment and/or services to originate calls from locations outside of the intercept subjects' normal service area and/or away from the normal intercept access

point. An example is "roaming" from an intercept subject's home cellular radio service area. Law enforcement still needs access to the electronic communications and related call setup information in these cases.

As electronic communications networks evolve into more interoperable (or even seamless) networks, future techniques for supporting law enforcement's intercepts should provide for an intercept access point that accommodates the mobility of the intercept subjects and/or their terminal equipment, which is associated with the intercept subjects by a number or other identifier. To ensure continuous access to communications, service providers should coordinate the routing of electronic communications and related call setup information such that communications and call setup information can be directed (e.g., routed or caused to be routed) to the intercept access point. If need be, court orders for multiple service providers can be obtained and served to satisfy any legal concerns related to communications or information routing.

In situations where the intercept subject invokes a call forwarding feature, law enforcement needs access to communications intended for a targeted telephone number or other identifier concurrent with the delivery of the communications to the "forwarded" destination. Law enforcement also needs the call setup information that identifies the final (forwarded) destination. For example, if an incoming call is forwarded from a *subscriber's* business number to his/her cellular phone number, law enforcement needs to know the cellular phone number (i.e., the number that calls are forwarded to and received). Law enforcement also needs to collect the number or other identifier of intermediate points if a call is forwarded multiple times before completing.

To collect both call setup information and call content, it may be necessary for law enforcement to have access to information on both signaling and communications channels associated with any given intercept.

The service provider will not be expected to monitor nor interpret the communications originated or received by the intercept subjects. It is law enforcement's responsibility to process the intercepted communications.

(R)-2 Law enforcement requires a *real-time, full-time monitoring* capability for intercepts.

- Law enforcement requires a real-time, full-time monitoring capability for call setup information plus call content intercepts.

- Law enforcement requires a real-time, full-time monitoring capability for call setup information only intercepts.

- When other than real-time acquisition of call setup information is sufficient, law enforcement requires the information to be available immediately upon call completion.

Electronic surveillance statutes specify that law enforcement must attempt to limit the communications intercepted to those relevant to the investigation. To satisfy this obligation, law enforcement must be able to monitor call content in real time.

(R)-3 Law enforcement requires service providers to be able to transmit intercepted communications to a *remote law enforcement monitoring facility*, away from the intercept access point and/or the intercept subjects' terminal equipment.

- To minimize the types of intercept monitoring equipment needed by law enforcement, the format for transmitting the intercepted communications to a remote law enforcement monitoring facility should be a generally available format.

- Law enforcement requires that call setup information and call content received at the remote law enforcement monitoring facility be the same as the information transmitted through the intercept access point.

Law enforcement may need the intercepted communications to traverse long distances from the intercept access point to the remote law enforcement monitoring facility. In some cases, coast-to-coast transport may be required. Service providers are expected to determine the type of *communications facility* needed to transmit the intercepted communications to the remote monitoring facility. In cases where intercepted communications must be carried across local access and transport area boundaries, law enforcement will acquire the appropriate services to permit *transmission* to the remote monitoring facility.

Intercepted call setup information and call content received at the remote monitoring facility should be the same as that transmitted through the intercept access point. In addition, the intercepted communications should arrive at the law enforcement monitoring facility in a generally available format (e.g., analog voice channel on a local loop, D4 formatted T-1 circuit, ISDN Primary Rate Interface circuit).

(R)-4 Law enforcement requires 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.

- The intercept shall remain transparent to the intercept subjects.
- The intercept shall remain transparent to parties called by or calling the intercept subjects.
- The intercept shall remain transparent to other subscribers and to service provider personnel, including *network management* and maintenance personnel, except as required to support the intercept or as otherwise authorized by the security manager, or equivalent, of the service provider.

Law enforcement requires service providers to restrict access to information about planned, ongoing or past electronic surveillance. Service providers shall not alert the intercept subjects or any other person to service changes requested by law enforcement to implement the intercept, unless systems security or maintenance requires disclosure or where otherwise required by law. Only those personnel with a need-to-know should have access to information about intercepts.

Service providers are not expected to ensure *transparency* beyond the capabilities of their own equipment. There may be cases where the intercept subjects have sophisticated equipment on their premises for detecting interception. To meet transparency requirements, the services provided to intercept subjects or any other subscribers should continue to comply with industry performance standards and limits.

(R)-5 Prior to intercept implementation and during the intercept, law enforcement requires (1) information from the service provider to verify the association of the communications acquired at the intercept access point with the intercept subjects, and (2) information on the services and features subscribed to by the intercept subjects.

Law enforcement must ensure that the intercepted communications relate to the intercept number or other identifier, and hence to the intercept subjects. Specifically, law enforcement must verify that the communications facility or service being intercepted corresponds to the subject or subjects identified in the court order. To accomplish the *verification*, law enforcement needs service provider information such as billing and caller identification information.

Service providers are expected to provide only information they receive and possess as part of their normal course of business. Service providers are not expected to provide information about the type of communications (facsimile, electronic mail, etc.) or the customer premises equipment that intercept subjects use for a call. For example, a service provider may be unable to determine the type of communications transmitted over an ISDN facility (e.g., facsimile transmission or voice communications). This situation may occur with any facility that allows the subscribers to use multiple types of terminal equipment and services.

While an intercept is ongoing, service providers should supply law enforcement with information on changes to the services and features subscribed to by the intercept subjects if requested by law enforcement. If these changes affect law enforcement's intercept capability, service providers should work with law enforcement to maintain access to the communications derived from calls to and from the targeted number or other identifier of the intercept subjects and/or their terminal equipment. Examples of services and features include follow-me roaming in cellular systems, ISDN services, call forwarding, caller identification, and speed dialing.

(R)-6 Law enforcement requires 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.)

Law enforcement needs to be able to perform multiple, simultaneous intercepts within a given service provider's system, central office, area, etc. Law enforcement and industry have historical data to use in estimating intercept demand. Projections may be stated as a percentage of the subscriber base of the individual service provider, the number of line terminations, or some other parameter.

Law enforcement expects the typical duration of call setup information only intercepts to range from 60 to 180 days, and the typical duration of call setup information plus call content intercepts to range from 30 to 90 days. However, there will frequently be circumstances where law enforcement needs to extend the court order beyond the above mentioned time frames. The expected duration of intercepts should be considered when forecasting intercept demand.

Law enforcement may need service providers to have reserve intercept capacities to meet unexpected increases above projections. During equipment and software design and development, industry should consider modular expansion capabilities or the identification of specific network nodes for use in all intercepts. As a goal, law enforcement and industry should work together to achieve a "no held order" operating environment (i.e., an environment where all intercept orders are fulfilled by service providers).

(R)-7 Law enforcement requires service providers to expeditiously provide access to the communications of the intercept subjects.

- Under routine circumstances and cases where no special *inside or outside plant construction* is necessary, access to the communications of the intercept subjects should be provided to the law enforcement monitoring facility in 24 hours or less from the delivery of the court order to the service provider.

- When special inside or outside plant construction is required, access to the communications of the intercept subjects should be provided to the law enforcement monitoring facility within 5 business days or as determined feasible by the service providers.

- In *emergency situations*, law enforcement requires access to the communications of the intercept subjects as soon as possible (i.e., within a few hours).

"Emergency situations" are typically life or death, national emergency, or other time-critical situations. "As soon as possible" may entail allowing law enforcement access to service provider facilities if sending information to a law enforcement monitoring facility will cause unacceptable delays. Law enforcement will continue to provide service providers with as much prior notification as possible.

(R)-8 Over the intercept period, law enforcement requires that the *reliability* of the services supporting the intercept at least equals the reliability of the communication services provided to the intercept subjects.

Law enforcement needs the service provider to take precautions to prevent potential problems from arising that may affect the reliability of the intercept. Routine maintenance and network management procedures, such as software upgrades, should not compromise the intercept or negate the ability to perform electronic surveillance.

In a multivendor service environment, isolating problems and ensuring reliability may require coordination and cooperation among the service providers involved in providing the intercept capability.

(R)-9 Law enforcement requires the *quality of service* of the intercepted transmissions forwarded to the monitoring facility to comply with the performance standards of the service providers.

Law enforcement expects the services provided for electronic surveillance purposes (e.g., leased lines) to have the same level of quality as services provided to the intercept subjects. Examples of quality of service parameters are call setup time, call blocking probability, signal-to-noise ratio, and bit error rate.

4. REFERENCES

General Services Administration, *Telecommunications: Glossary of Telecommunication Terms*, Federal Standard 1037B, 3 June 1991.

Institute of Electrical and Electronics Engineers, *IEEE Standard Dictionary of Electrical and Electronics Terms*, American National Standards Institute/IEEE Standard 100-1988, Fourth Edition, 1988.

United States Code (U.S.C.), Title 18, Chapter 119, "Wire Interception," Section 2510, "Definitions."

U.S.C., Title 18, Chapter 119, "Wire Interception," Section 2518, "Procedures for Interception of Wire, Oral, or Electronic Communications."