

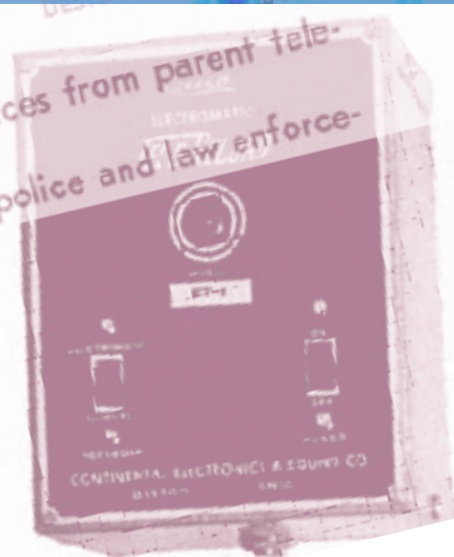
Technical Aspects of Lawful Interception

ITU-T Technology Watch Report #6

May 2008

NEW
NOW
Telephone
SURVEILLANCE
WORK MADE EASY

- ★ Makes telephone recordings automatically
- ★ No Attendant necessary
- ★ Adaptable to most any recorder
- ★ Can be used near or great distances from parent telephone
- ★ Now being used successfully by police and law enforcement agencies nationally



Technical Aspects of Lawful Interception

ITU-T Technology Watch Report 6
May 2008

In this report, Lawful Interception (LI) describes the lawfully authorized interception and monitoring of telecommunications pursuant to an order of a government body, to obtain the forensics necessary for pursuing wrongdoers. LI has existed from the times of shortrange telegraphy to today's worldspanning Next-Generation Networks (NGNs). The report studies the technical concepts underlying LI, and describes existing standardization done in this field.

ITU-T Technology Watch Reports are intended to provide an up-to-date assessment of promising new technologies in a language that is accessible to non-specialists, with a view to:

- Identifying candidate technologies for standardization work within ITU.
- Assessing their implications for ITU Membership, especially developing countries.

Other reports in the series include:

- #1 [Intelligent Transport System and CALM](#)
- #2 [Telepresence: High-Performance Video-Conferencing](#)
- #3 [ICTs and Climate Change](#)
- #4 [Ubiquitous Sensor Networks](#)
- #5 [Remote Collaboration Tools](#)
- #6 [Technical Aspects of Lawful Interception](#)
- #7 [NGNs and Energy Efficiency](#)

Acknowledgements

This report was prepared by Martin Adolph (tsbtechwatch@itu.int) with Dr Tim Kelly. It has benefited from contributions and comments from Anthony M. Rutkowski.

The opinions expressed in this report are those of the authors and do not necessarily reflect the views of the International Telecommunication Union or its membership.

This report, along with other Technology Watch Reports can be found at www.itu.int/ITU-T/techwatch.

Please send your comments to tsbtechwatch@itu.int or join the Technology Watch Correspondence Group, which provides a platform to share views, ideas and requirements on new/emerging technologies and to comment on the Reports.

The Technology Watch function is managed by the ITU-T Standardization Policy Division.

Technical Aspects of Lawful Interception

1 Interception (circa. 1844)

The establishment of the International Telecommunication Union (ITU) on 17 May 1865 (originally named International Telegraph Union¹) was closely linked with the invention of the telegraph. Already, some 20 years earlier, Samuel Morse had sent the first public message over a 61 km telegraph line between Washington and Baltimore, and through that simple act, he ushered in the telecommunication age. Since those early days of electronic communications², communicating parties have come to expect that their messages one to another will remain private. Indeed,

ITU treaties provide the basic legal text, incorporated into the national legislation of many countries that establishes the principle of secrecy of telecommunications. But the ITU basic texts also provide the legal basis for lawful interception forensics in order to apply national laws and international conventions.³ It is the technical implementation of those two opposing requirements – secrecy and forensics – that is the topic of this report (See Box 1).

Box 1: Lawful Interception and Wiretapping in different eras of telecommunication

Telegraph era

Telecommunication technologies were first created around 1840, and one of the earliest instances of telegraphic interception reportedly occurred in 1867, when a Wall Street stockbroker collaborated with Western Union telegraph operators to intercept telegraph dispatches sent to Eastern newspapers by their correspondents in the West. The intercepted messages were then replaced by counterfeit ones which reported bankruptcies and other financial disasters supposedly befalling companies whose stock was traded on the New York Stock Exchange. When the share prices were driven down, the wiretappers then purchased their victim's stock.⁴

Telephone era


Magazine ad (1962) for easy telephone surveillance with *Tel-O Record*.⁵

Digital network era

During the 1990s, law enforcement struggled with the large-scale conversion of telecommunications to digital formats and equipment, including internet platforms. This resulted significant new legislation, standards cooperation and products in nearly every country and region to provide the forensic capabilities that previously existed.

Adapted from various sources.

NEW



NOW
Telephone
**SURVEILLANCE
WORK MADE EASY**


- ★ Makes telephone recordings automatically
- ★ No Attendant necessary
- ★ Adaptable to most any recorder
- ★ Can be used near or great distances from parent telephone
- ★ Now being used successfully by police and law enforcement agencies nationally

An Electronic Transistorized control unit for automatically controlling the manual operating functions of any standard sound recording machine to record sound from telephone line. Unit will operate from any recording machine which has sufficient torque to start in record position. Will work satisfactorily on any national or foreign telephone single or multiple line system. Recorder runs only when telephone is in use. Automatically starts when telephone is answered or used for calling. Automatically stops when telephone call is completed. May be used on off premise extension as distant as five miles from parent phone by direct parallel connections. Can also be used to detect numbers called by the click method. Cannot be detected or heard by parent phone. Operates from self-contained power supply 115 volt A.C. 60 cycle.

See your Industrial Electronic Distributor or use the Readers Service card for catalogue and your nearest distributor.

Export Division: EMEC, Inc.
127 Grace St. Plainview, L.I., N.Y.

DESIGN PATENT 30220601



NET PRICE
\$79.95

NOTE: Not intended for automatic telephone answering.

In this report, **Lawful Interception** (LI) describes the lawfully authorized interception and monitoring of telecommunications pursuant to an order of a government body, to obtain the forensics necessary for pursuing wrongdoers. It is a need that has existed from the times of short-range telegraphy to today's world-spanning Next-Generation Networks (NGNs).

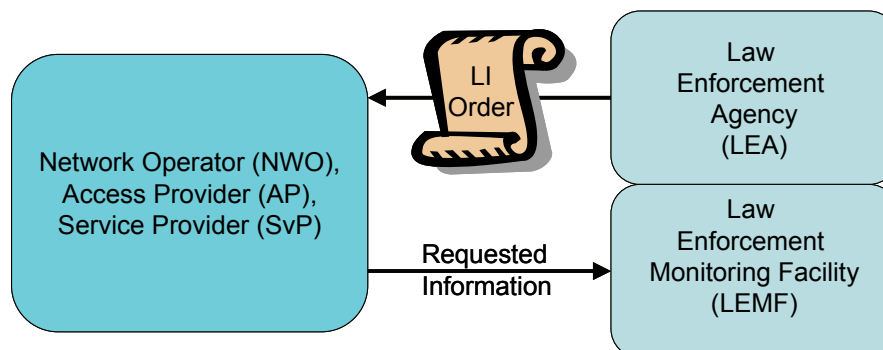
LI and the question how to deal with this topic have recently been discussed in different ITU-T Study Groups. This report, the sixth in a series of ITU-T [Technology Watch](#) briefing papers, will focus on the technical concepts underlying LI, and describes existing standardization done in this field.

2 When is interception lawful?

For interception to be *lawful*, it must be conducted in accordance with national law, following due process after receiving proper authorization from competent authorities. Typically, a national Law Enforcement Agency (LEA) issues an order for LI to a

specific network operator, access provider, or network service provider, which is obliged by law to deliver the requested information to a Law Enforcement Monitoring Facility (LEMF: See Figure 1).

Figure 1: Organizational flow chart for Lawful Interception



Source: Adapted from ETSI TS 101 331, Definition of interception.
See www.pda.etsi.org/pda.

In order to prevent investigations being compromised, national law usually requires that LI systems hide the interception data or content from operators and providers concerned. Whilst the detailed requirements for LI differ from one jurisdiction to another, the general requirements are similar: The LI system must provide transparent interception of specified traffic only, and the intercept subject must not be aware of the interception. Additionally, the service provided to other uninvolved users must not be affected during interception. The term *subject*, as used here, can refer to one person, a group of persons, or equipment acting on behalf of persons, whose

telecommunications are to be intercepted. Lawful interception also implies that the subject benefits from domestic legal protection. However, protections are complicated by cross-border interception.

Decades ago, LI was typically performed by applying a physical 'tap' on the targeted telephone line, usually by accessing digital switches of service providers. As the infrastructure converted to new digital network and services formats, LI standards and systems were adapted to keep pace with the new deployments. In bringing about this transition, the principal concern of operators was the question of "who pays?" Different nations have chosen means appropriate to their environment.

3 Common architecture

LI may target two types of data: the actual contents of communications (CC) which may include voice, video or text message contents, and Intercept Related Information (IRI, Call Data (CD) in the United States). IRI consists of information about the targeted communication itself: signalling information, source and destination (telephone numbers, IP or MAC addresses, etc), frequency, duration, time and date of communications. On mobile networks, it may also be possible to trace the geographical origin of the call.⁶ Network operators have always been collecting some IRI for billing and network management purposes and so it is relatively easy for law enforcement agencies to gain access to this information, under *subpoena*.

The act of LI – independent of the type of communication to be intercepted – may logically be thought of as a process with three distinct steps:

1. *Capture* – CC and IRI related to the subject are extracted from the network.
2. *Filtering* – information related to the subject that falls within the topic of the inquiry is separated from accidentally gathered information, and formatted to a pre-defined delivery format
3. *Delivery* – requested information is delivered to the LEMF

Capture and filtering may be facilitated by the use of the latest speech technologies: Speaker identification, along with language and gender recognition, combined with real-time keyword-spotting, can be performed by specialized servers devoted to collecting, analyzing and recording millions of incoming calls as soon as they are intercepted. This can free operators to carry out more specialized tasks requiring a higher level of identification and analysis.

However, enabling secure private communications for its customers still remains the primary purpose of service providers. To prevent this service being adversely affected by LI, the network architecture requires that there be distinct separation between the Public Telecom Network (PTN) and the Law Enforcement

Network, with standardized interfaces that manage the hand-over of data between both networks. Three functions are responsible for the work within the PTN:

- The Administration Function (ADMf) receives interception orders from the LEA and hands them over to
- Internal Intercept Functions (IIF), which are located tactically within network nodes and generate the two desired types of information, CC and IRI.
- Mediation Functions (MF) take charge of delineation between the two networks. They implement Internal Network Interfaces (INI), which may be proprietary, to communicate within the PTN, and standardized interfaces, to deliver requested information to one or more LEMFs.

Figure 2 provides a more comprehensible overview of networks, functions, and interfaces within a generalised LI architecture.

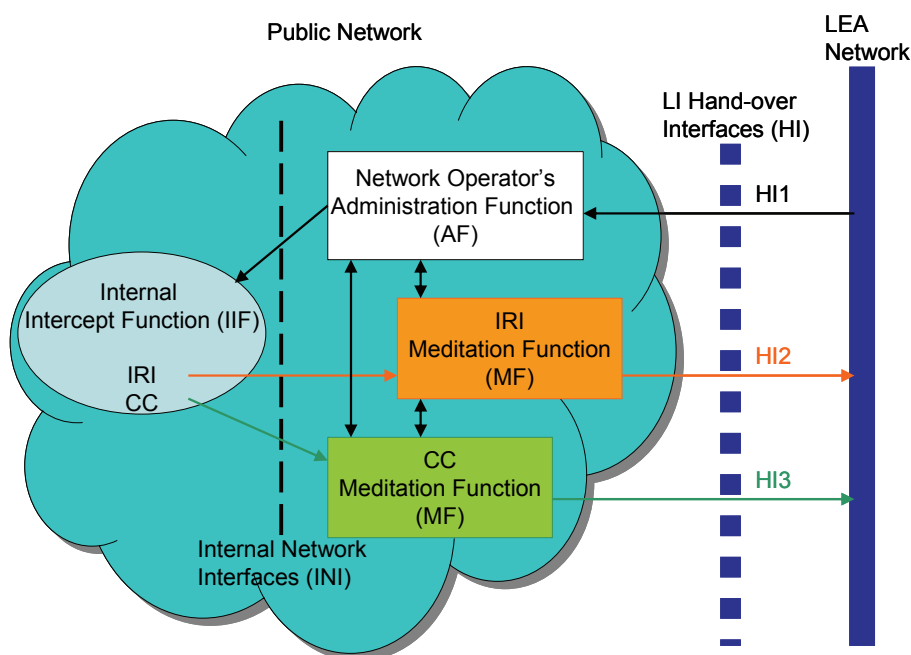
For calls made over IP networks rather than the PSTN, things look slightly different⁷: Each call consists of one or more call-signalling streams that control the call, and one or more call-media streams which carry the call's audio, video, or other content, along with information concerning how that data is flowing across the network. Together, these streams make up a so called "session". As individual packets of data within a session might take different paths through the network, they may become hard to relate with each other. In Voice over Internet Protocol (VoIP) networks, a device named a Session Border Controller (SBC) plays the role of exerting influence over the data streams that make up one or more sessions.

The word *Border* in SBC refers to the demarcation line between one part of a network and another, which is a strategic point to deploy Internal Intercept Functions, as both targeted types of data – IRI and the corresponding CC – pass through it. This architecture is equally applicable to other IP-based services, where the IRI contains parameters associated with the

type of traffic from a given application to be intercepted. In the case of e-mail, IRI conforms to the header information of an e-mail message. The header usually

contains the source and destination e-mail addresses and information about the time the e-mail was sent.

Figure 2: Generalised view of the Lawful Interception architecture



Source: Adapted from ETSI TS ES 201 158.

4 Standardization activities

Service providers and vendors are being asked to meet legal and regulatory requirements for the production of forensics in a variety of countries worldwide. Although requirements may vary from country to country⁸, most requirements remain common.

The principal global forums for specifying the requirements as well as specific standards are the European Telecommunication Standards Institute (ETSI) Technical Committee on Lawful Interception (TC LI) and the 3rd Generation Partnership Project (3GPP). New NGN LI standards are being developed through ETSI TISPAN in collaboration with TC LI and 3GPP. Most of the world uses these standards. Notable exceptions include the USA CALEA related standards, and the Russian Federation SORM specifications. In

addition, [Cable Television Laboratories](#) develops generic standards of cable system use.

Common forensic standards are effectively encouraged by the international [Convention on Cybercrime](#) maintained by the Council of Europe which currently has 45 signatories – a number of which are outside Europe.⁹ For a majority of the signatories, their legislation requires technologies based on standards developed by TC LI and [3GPP SA WG3](#).

In [RFC 2804](#), the Internet Engineering Task Force (IETF) feared that, by implementing interception functionality, a system would be less secure and more complex than it could be had this function not been present. It noted that, being more complex, the risk of unintended security flaws in the system

would become larger.¹⁰ [RFC 3924](#), which was published subsequently, describes Cisco's Architecture for Lawful Intercept in IP Networks.

Lawful Interception intersects with technology, network management and operational aspects of all types of telecommunications, and could therefore be an item on the agenda of several Study

Groups (SGs), Focus Groups and Global Standards Initiatives (GSI) within ITU-T. However, LI is treated with differing priorities and intensity with some groups deciding that it is out of scope. Some view LI as a national rather than an international matter while others fear that ITU efforts would be duplicative of work elsewhere, notably in ETSI TISPAN.

Box 2: Lawful Interception Standards published by ETSI

The purpose of standardizing of lawful interception in ETSI is to facilitate the economic realization of lawful interception that complies with the national and international conventions and legislation. Examples of standards include:

- ES 201 671 Handover Interface for the Lawful Interception of Telecommunications Traffic (revised).
- ES 201 158 Requirements for Network Functions
- TS 102 234 Service-specific details for Internet access services
- TS 102 233 Service-specific details for e-mail services
- TS 102 232 Handover Specification for IP Delivery
- TS 102 815 Service-specific details for Layer 2 Lawful Interception
- TS 101 331 Requirements of Law Enforcement Agencies
- TR 102 053 Notes on ISDN lawful interception functionality
- TR 101 944 Issues on IP Interception
- TR 101 943 Concepts of Interception in a Generic Network Architecture

Source: Adapted from www.portal.etsi.org/li/Summary.asp.

5 Market Watch

For companies providing LI technology and services, the increasing numbers of people worldwide with access to telecommunications, steadily advancing telecommunication technologies, and frequently-amended laws, are both a challenge and a blessing. The customers for LI services include LEAs, national security agencies, or - where a private corporate or government network facility is involved - the party responsible for this network.

The number of interception applications authorised by LEAs continues to increase worldwide (especially in countries that maintain extensive surveillance capabilities). Besides lawful interception systems, other network forensics facilities, such as data

retention technologies for the collection and storage of intercept related information of all communications, have to be installed by service providers in a growing number of states worldwide. These network management and forensics solutions are developed and sold by a huge number of suppliers from different countries. Some of them have formed a global industry forum (the Global LI Industry Forum ([GLIIF](#))) to promote worldwide awareness, responsible development and market growth for LI products and services. LI solutions on the market are necessarily compliant with either the ETSI Standards for most countries, plus SORM in Russia and CALEA in the U.S.

6 Conclusion

Information and communication technologies have supported Lawful Interception since the era of Morse's telegraph. Interception is actively practiced worldwide with an increasing number of

applications. Accurate international standards-based network forensics technologies for lawful interception, data retention and network management are needed to meet national requirements.

Glossary of abbreviations and acronyms used in the document

3GPP	3rd Generation Partnership Project
ADMF	Administration Function
AP	Access Provider
CALEA	Communications Assistance for Law Enforcement Act
CC	Contents of Communications
CD	Call Data
ETSI	European Telecommunications Standards Institute
ICT	Information and Communication Technology
IIF	Internal Intercept Function
INI	Internal Network Interface
IRI	Intercept Related Information
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication standardization sector
LEA	Law Enforcement Agency
LEMF	Law Enforcement Monitoring Facility
LI	Lawful/Legal Intercept/Interception
MAC	Media Access Control
MF	Meditation Functions
NGN	Next-Generation Network
NWO	Network Operator
PSTN	Public Switched Telephone Network
PTN	Public Telecom Network
QoS	Quality of Service
SA	Services & System Aspects
SBC	Session Border Controller
SvP	Service Provider
TC LI	Technical Committee on Lawful Interception
TISPAN	Telecoms & Internet converged Services & Protocols for Advanced Networks
VoIP	Voice over Internet Protocol
WG	Working Group

Notes, sources and further reading

- ¹ To find out more about ITU's history, see www.itu.int/net/about/history.aspx.
- ² Of course, interception of messages predates the electronic age. In the Napoleonic wars, interception of semaphore signals was common, while in the Elizabethan era, breaking of secret codes and ciphers played a key role in the events that led to the execution of Mary Queen of Scots (see, for instance, Budiansky, S. (2000) "Battle of Wits"). But the intention here is to focus on lawful interception of telecommunications.
- ³ The relevant text is, *inter alia*, in [Article 37](#) of the ITU Constitution, which states:
 - a. *Member States agree to take all possible measures, compatible with the system of telecommunications used, with a view to ensuring the secrecy of telecommunications.*
 - b. *Nevertheless, they reserve the right to communicate such correspondence to the competent authorities in order to ensure the application of their national laws or the execution of international conventions to which they are parties.*

In addition to Article 37 of ITU's Constitution, as cited above, Article 41 grants priority treatment to government telecommunications.
- ⁴ See Peter N. Grabosky and Russell G. Smith, "Crime in the Digital Age: Controlling Telecommunications and Cyberspace Illegality," 1998; www.books.google.com/books?id=7_z4Ihh49wAC&hl=en.
- ⁵ See www.spybusters.com/History_1962_Wiretap_ad.html.
- ⁶ See Newport Networks, "Lawful Interception Overview," 2006; www.newport-networks.com/whitepapers/lawful-intercept1.html.
- ⁷ See A. Rojas, P. Branch, "Lawful Interception based on Sniffers in Next Generation Networks," Australian Telecommunications Networks & Applications Conference 2004, Sydney, Australia, December 8-10, 2004; www.caia.swin.edu.au/pubs/ATNAC04/rojas-branch-2-ATNAC2004.pdf.
- ⁸ See SS8 Networks, "The Ready Guide to Intercept Legislation 2;" www.ss8.com/ready-guide.php.
- ⁹ See Council of Europe, ETS No. 185, Convention on Cybercrime. Title 5 – Real-time collection of computer data. Articles 20 and 21. www.conventions.coe.int/Treaty/EN/Treaties/Html/185.htm. The Convention has been signed by 45 Member States and non-Member States, see www.conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=1&DF=9/2/2006&CL=ENG.
- ¹⁰ See Susan Landau, "Security, Wiretapping, and the Internet," *IEEE Security and Privacy*, vol. 3, no. 6, pp. 26-33, Nov/Dec, 2005. Also see Vassilis Prevelakis and Diomidis Spinellis, "The Athens Affair," *IEEE Spectrum*, July, 2007; www.spectrum.ieee.org/print/5280.



www.itu.int/itu-t/techwatch