NetOptics®

Gaining Total Visibility for Lawful Interception

White Paper

This paper provides a basic definition and description of Lawful Interception (LI), as well as offering a brief overview of current challenges that confront communications organizations and law enforcement. The paper also evaluates some technology options for organizations in monitoring digital and voice communications across diverse channels.

LI encompasses all activities that affect the capture and storage of digital and voice communications traveling over the network of a service provider, including the telephone and the Internet.

Each country has its own criteria for defining criminal or terrorist activities; the purpose of LI is to gather evidence to detect and prevent such activities. In the United States, the Communications Assistance for Law Enforcement Act (CALEA) sets forth how service providers must support lawful interception. Abroad, the European Telecommunications Standards Institute (ETSI) drives adoption of standards for telecommunications, broadband, and related technologies in Europe and other countries.

The Purposes of Lawful Interception

LI is intended to obtain certain communications network data for the purposes of analysis, or for use as evidence, pursuant to legal authority. Such data might take the form of signaling or network management information or may include the actual content of the communications. If data is not obtained in real time, LI activity is referred to as “access to retained data”.

The term “lawful interception” describes the process by which law enforcement agencies conduct electronic surveillance of circuit and packet-mode communications as authorized by judicial or administrative order.

To protect the common welfare, nations worldwide have adopted legislative regulations mandating that communications providers design their networks in such a way as to enable authorized electronic surveillance. International standards organizations set forth parameters to guide service providers (SPs) and manufacturers in implementing these standards.

Most people are aware of surveillance in the form of “wiretaps” on traditional telecommunications such as telephones. As communication technologies have become more complex, interception techniques have grown accordingly. Nowadays, the idea behind wiretapping is also employed in voice, data, and multiservice networks that deliver Internet services. Figure 1 illustrates the variety of communications that can be monitored, including voice over IP (VoIP), email, Web traffic, file sharing, and so forth.

“Wiretapping “ in the Digital Age

Wiretapping applied to digital media differs in process but not in either intent or concept from analog. Under LI, a Law Enforcement Agency (LEA) will decide to perform electronic surveillance on a “target,” under the authorization of a judge or other authority. Surveillance is implemented by means of wiretaps on traditional telecommunications and by digital intercepts on Internet services in voice, data, and multiservice networks.

The LI process may be handled by a third-party vendor using its own proprietary mediation device. Such a device not only provides the interface that LI uses for interception but can also create requests to other network devices to carry out the LI. Lastly, the mediation device can convert the traffic into the format required by the LEA, which can vary by country or by governmental agency.

The LEA. after demonstrating legally mandated probable cause, might deliver a request for a wiretap to the SP of the entity under investigation. That SP then uses the target’s Internet Protocol (IP) address to determine which of its edge routers handles the target’s traffic in the form of data communication. The SP intercepts suspect traffic as it passes through the router and sends a copy to the investigative agency without the awareness of the entity under investigation.

The need for accuracy and reliability of the information is difficult to overstate, because the consequences of surveillance may be profound, both for the target and for law enforcement itself.

The LI Monitoring Infrastructure: Concepts and Components

The technology of LI monitoring is driven foremost by the changing needs of law enforcement—which in turn respond to the fast-evolving Internet and the nature of the threats. As a result, a variety of solutions has emerged to address diverse applications such as homeland security and may require information delivered in specific formats. Because intercepts on the network must be secret, the active intercept messages have to be kept separate from messages used for routine call setup.

At its most fundamental level, LI monitoring technology consists of a listening device placed on the telephone or computer cable—a process conducted in accordance with the requisite legal permissions for

interception—plus a device to record and alert authority when trigger points are reached. For example, a CALEA for Voice feature would allow the lawful interception of voice conversations running on VoIP. When a law enforcement entity wishes to monitor a telephone conversation, CALEA for Voice would make copies of IP packets carrying the conversation and send duplicates to respective monitoring devices.

Telephone interception and monitoring

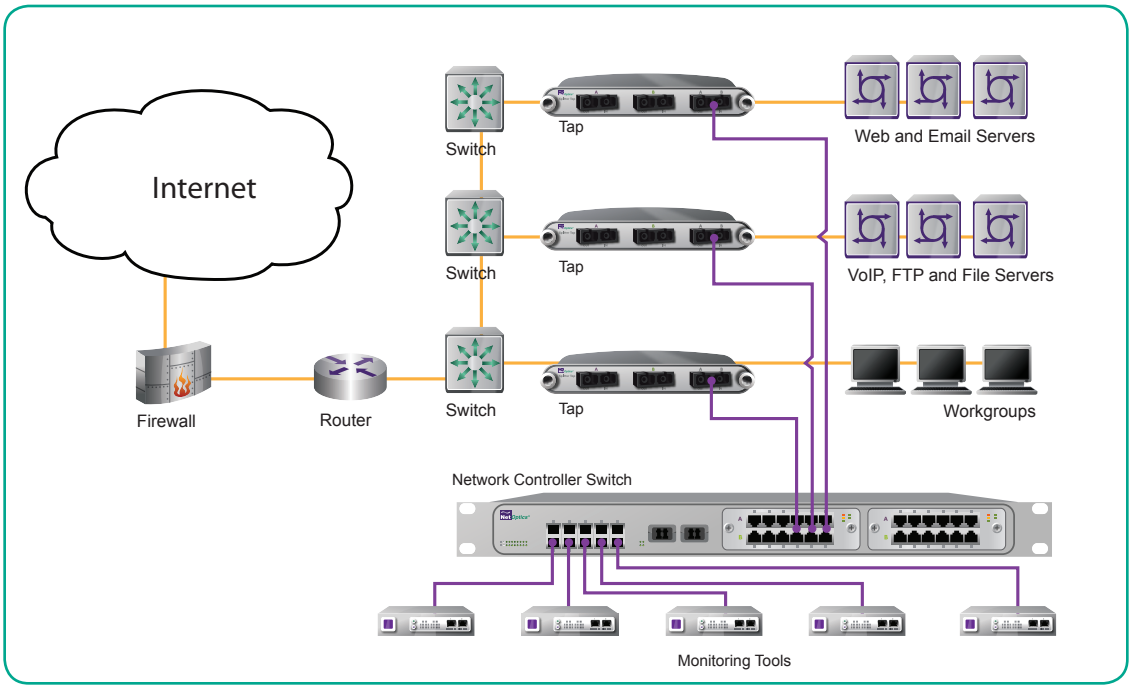
Telephone conversations may be recorded in their entirety, or in a form determined by the need of the specific legal instance: For example, recording might be confined to outgoing conversations only, or to solely international calls. Some messages are audited in real time and only recorded and stored if content of a suspicious nature becomes evident in a short period of time.

Pen Register or Trap and Trace devices record or decode dialing, routing, addressing, or signaling information, but do not include the contents of any communication. They take note only of calls and data similar to that which appears on a phone bill, such as time of call, answer, disconnect, and call forward information.

Computer Traffic Monitoring

In the U.S., LI capabilities on the Web are legally mandated by the Communications Assistance for Law Enforcement Act (CALEA). This is because computer-to-computer communication presents a huge volume of information and potential threats, with so many people and entities connecting to Web sites, email servers, ISPs, and file servers daily. LEAs can filter this information for authentic threats by tracking users; or by tracking the data itself that is transferred; or by noting traffic patterns. Following is a list of primary activities that can be monitored:

- **Web site use tracking**
  When a user connects to a Web site, the site can record the IP address that the user connected from and the one that he or she connects to afterwards. LEA can also track this activity.
- **Email**
  Email typically passes through many intermediary sites between sender and receiver. These sites



Taps and a Network Controller Switch provide invisible, transparent access to digital communications for LI applications

can consist of any page on the Internet, the Internet Service Provider, Web-hosting services, and the email provider. Email messages can be intercepted in or between any of these sites.

- **Instant Messenger (IM)**
  Instant Messenger-type correspondence is sent from the IM originator's computer to a server, and from there to the recipient's computer.
- **File Transfer**
  File transfer moves data from one computer to another, typically over the Internet. Since all files travel in packets sent over an IP-based network, any type of file can be transferred: music downloads, data storage, or tax payments.

Encryption

Users can encrypt some telephone conversations and most computer transmissions. However, unless the user performs this encryption very carefully, using sophisticated, strong keys, the data may be vulnerable to decryption, given enough computing power and time. LEAs can also send encrypted data to forensic specialists for decryption, if they deem that necessary.

Functional Requirements for a Lawful Interception Device

For an LI device to function effectively, it should embody the following feature set:

- *Undetectability and unobtrusiveness.* Neither the initiator or recipient of a communication should be able to detect the presence of the LI device. The LI device should passively record all network transactions and not alter any part of the network traffic.
- *Real-time monitoring capabilities.* Because of the nature of law enforcement, timing is of the utmost importance in preventing a crime or an attack or in gathering evidence.
- *Complete visibility into network traffic.* This includes:
  - 100 percent visibility at any point in the communication stream
  - Zero dropped packets: This is particularly important with encryption, where missing characters can render a message incomplete or unreadable.
- Adequate processing speed. This must be sufficient to match network bandwidth.

Net Optics: a Range of Solutions for Lawful Interception

Test access ports, or Taps are devices used by carriers and others to meet the capability requirements of CALEA legislation. Net Optics Taps reside in both carrier and enterprise infrastructures to carry out network monitoring and to improve both network security and efficiency. These devices are placed in-line to provide permanent, passive access points to the physical stream. That passive characteristic of Taps means that the network data is unaffected, whether the Tap is powered or not. As part of an LI solution, Taps have proven more useful than Span ports. If LEA must reconfigure a switch to send the right conversations to the Span port every time intercept is required, a risk arises of misconfiguring the switch and connections. Also, Span ports drop packets—another significant monitoring risk, particularly in encrypted communications.

Director Xstream™ and iLink Agg Xstream™ enable deployment of an intelligent, flexible and efficient monitoring access platform for 10G networks. Director Xstream's unique TapFlow™ filtering technology enables LI to focus on select traffic of interest for each tool, based on protocols, IP addresses, ports, and VLANs. The robust engineering of Director Xstream and iLink Agg Xstream enable a pool of 10G and 1G tools to be deployed across a large number of 10G network links, with remote, centralized control of exactly

which traffic streams are directed to each tool. Net Optics Xstream solution enables law enforcement to view more traffic with fewer monitoring tools, as well as relieve oversubscribed 10G monitoring tools. In addition, law enforcement can share tools and data access among groups without contention and centralize data monitoring in a network operations center.

Director Pro Network Controller switch provides law enforcement with Deep Packet Inspection (DPI) capabilities that enable an agency to hone in on a specific phone number or credit card number. The product differs from other platforms by offering a unique ability to filter content or perform pattern matching up through Layer 7. DPI provides the ability to apply filters to a packet or multiple packets at any location, regardless of packet length; how "deep" the packet is; or the location of the data to be matched within the packet.

With its history of leading innovation in monitoring and security solutions, Net Optics provides scalable, easy-to-use products designed to support Lawful Interception projects, users, and goals. The company offers equipment to telecoms and service providers who fall under the CALEA mandate, as well to LI solution resellers. Net Optics solutions are purpose-built for LI, offering the performance, visibility, and flexibility to perform the mission.

For further information about Tap technology for lawful interception applications:

http://www.netoptics.com
Net Optics, Inc.
5303 Betsy Ross Drive
Santa Clara, CA 95054
(408) 737-7777
info@netoptics.com

Distributed by:

Network Performance Channel GmbH
Ohmstr. 12
63225 Langen
Germany

+49 6103 906 722
info@np-channel.com
www.np-channel.com