## Challenges to Lawful Interception

With a worldwide landscape characterized by entirely new forms of electronic communication the nature of lawful interception (LI) has changed substantially.

Regulatory mandates implemented in many countries present a significant challenge to the telecommunications companies, network operators, and service providers tasked with meeting current requirements.

Solutions that have been developed in recent years to comply with local and national regulations differ considerably from the tools of past eras.

Today, the onus is on companies to modify and extend their network infrastructures to accommodate the necessary framework for lawful interception and to support techniques that permit the capture and analysis of communication data in response to law enforcement requests.

The complexities of today's communication environment heighten the need for lawful interception tools versatile enough to contend with the widest range of wired and wireless communication exchanges. These tools must also have the interoperability to integrate easily into existing network infrastructures as well as the reliability to meet real-world challenges in a proven and secure manner and consequently, effective solutions need to be available on demand to respond to all lawful surveillance requests from those agencies empowered by law to obtain the information.

## Regulatory Environment

An overlapping framework of international and national regulations establishes the foundation for the monitoring of telecommunications, implemented to enable law enforcement agencies to intercept messages or information being distributed for illegal purposes.

## National Laws

Throughout the world, regulations relevant to lawful interception continue to be updated and modified to contend with advances in telecommunications and evolving forms of voice and data communication. Although the regulatory environment and the nature of the solutions required for compliance vary from region to region, the overall intent in most cases is very similar and the tools that provide compliance share common characteristics.

In the United States, the Communications Assistance for Law Enforcement Act (CALEA), which was recently extended by a Federal Communications Commission (FCC) ruling to ensure that companies that provide VoIP services meet the compliance requirements stipulates the conditions under which telecommunications voice providers must assist a law enforcement authority in intercepting specific subscriber calls when presented with a valid court order.

**SSI Pacific Pty Ltd**
ABN 93 137 274 107 ACN 137 274 107
Level 1/620 Bourke Street Melbourne Victoria 3000 Australia
+61 3 9653 9163 +61 3 9653 9307 info@ssipacific.com

**www.ssipacific.com**

In the European Union, In a council resolutions enacted on January 17, 1995, the European Union specified requirements for national lawmakers and law enforcement agencies that establish the basis for various national telecommunication surveillance laws, as well as for many international interception standards.

The European Telecommunications Standards Institute The European Telecommunications Standards Institute (ETSI) has been a major driver in defining lawful interception standards, not only for Europe, but worldwide. Technical standards ratified by ETSI specify a general architecture for LI that allows systematic and extensible communication between network operators and LEAs over defined interfaces.

Mandatory compliance with this ETSI standard has been enacted in a number of countries; the provisions state that following the request of a valid authority, the results of a lawful interception of a particular individual shall be delivered to the appropriate law enforcement agency.

The 3rd Generation Partnership Project In addition to the ETSI specifications, a consortium of technology organisations called the 3rd Generation Partnership Project (3GPP) collaboratively defined technical specifications for lawful enforcement in 3G and future mobile networks. The initial applicable standards, 3GPP TS 33.106-108, establish a compliance framework that has been actively embraced by many industry participants (comparable to ETSI TS 101 331).

**Solution Considerations**

Ideally, a successful lawful interception solution must be flexible enough to adapt to varying regulations and interoperable enough to deploy easily within the diverse network infrastructures in different regions. Countries around the world have responded to the threats of terrorism and criminal activity by enacting legislation that provides the legal basis for lawful interception.

The differences from country to country essentially involve the specific requirements as defined by the legislation, including the communication services to be intercepted, the applicable data formats covered, and the mechanisms through which particular types of communication are to be handed over to law enforcement agencies (LEAs). In the United States, for example, Congress mandated that all telecommunication operators provide interception capabilities to LEAs.

Regardless of the specific geographic location, the prevailing regulatory environment in your region is likely to include provisions so that lawful interception operations can be performed when requested by an authority.

The following list highlights the capabilities of a lawful interception solution that are most relevant to regulatory mandates and legislative requirements.

- **Comprehensive interception capabilities:** The LI solution must be able to intercept all applicable communications of a certain target without any gaps in coverage.
- **Reliability and integrity:** The LI solution should ensure delivery of precise and accurate results with the highest levels of data integrity. The LI solution must be as reliable as the service to be intercepted
- **Separation of content:** Intercepted communications data should be divisible into individual components; for example, the metadata included in the Interception Related Information (IRI) should be separable from the Communication Content (CC).

**SSI Pacific Pty Ltd**
ABN 93 137 274 107 ACN 137 274 107

Level 1/620 Bourke Street Melbourne Victoria 3000 Australia
+61 3 9653 9163 +61 3 9653 9307 info@ssipacific.com

**www.ssipacific.com**

- **Transparent surveillance:** The monitoring activities performed by the solution must not be detectable by the subscriber.
- **Immediate activation and real-time responsiveness:** Following a request for lawful interception, a solution must be able to be immediately activated and provide real-time response in delivering intercepted data.
- **Sufficient capacity:** The solution must have adequate capacity to handle the scope and scale of requested surveillance activities.
- **Data security and privacy:** Sensitive data must be protected during transmission and the privacy of an individual's records and personal information should be safeguarded. Only authorised personnel should be able to view intercepted data.
- **Decryption:** Encrypted data shall be delivered in plain text format if the encryption keys are available to the service provider or network operator.
- **Complete logging of events:** All LI-related activities must be recorded and logged as part of a centralised record-keeping procedure.

**SSI Pacific Pty Ltd**
ABN 93 137 274 107 ACN 137 274 107

Level 1/620 Bourke Street Melbourne Victoria 3000 Australia
+61 3 9653 9163 +61 3 9653 9307 info@ssipacific.com

**www.ssipacific.com**