



WHAT IS LAWFUL INTERCEPTION?

17 June 2022

In the recent years, with the advancement of technology, legislatures around the world have created and introduced laws defining the legal framework and authority for their respective governments to perform interception.

The Telecommunications (Interception Capability and Security) Act (TICSA) was passed in New Zealand in November 2013. Under this Act, the police have the responsibility for maintaining a register of network operators that holds information, on behalf of all the surveillance agencies about network operators and their compliance with the obligations set out in the Act. Lawful interception implementation is required by majority of countries around the world to prevent crime and fraud.

This blog will aim to give a run through of the basics and importance of lawful interception.

What is interception?

Interception is the acquisition of communication content and data through the use of any electronic, mechanical or any other device. Legal or lawful interception (LI) is obtaining communications network data from a lawful authority for the purpose of analysis or evidence.

In New Zealand, under the TICSA, to intercept in relation to telecommunication, “includes hear, listen to, record, monitor, acquire or receive the telecommunication while it is taking place on a telecommunications network; or while it is in transit on a telecommunications network.” Surveillance agencies can only undertake an interception when acting under a lawful interception power or authority.

By law, internet service providers (ISPs) and telecommunication companies must be able to intercept and relay network traffic to law enforcement, in real time and by specific standards when presented

with a warrant. LI solutions are important for their usefulness in providing real time data and interception in preventing, detecting, deterring, and prosecuting criminal acts.

How do I know if I am compliant?

Many network operators have a regulatory requirement to incorporate lawful interception capabilities into their networks so that Law Enforcement Agencies (LEAs) can commission authorized electronic surveillance of specific network users.

Under TICSA all network operators must register their information with the New Zealand Police Registrar. A network operator is defined in the legislation as “a person who owns, controls, or operates a public telecommunications network; or a person who supplies another person with the capability to provide a telecommunications service.” It is the responsibility of the network operator to know if the company is compliant. A designated officer may require certification and/or testing to be carried out. Companies in breach of lawful intercept obligations face fines upward of \$50,000 per day.

Basic requirements of a lawful interception solution

The details of LI solutions differ between the different types of interceptions but there are some basic requirements that every LI solution must have. A LI solution must provide transparent interception of only the specific traffic, and the subject must not be aware of the interception. During an interception operation, the telecommunication users must not be affected in any way by degrading their provisioned service. Additionally, in every interception there are minimum data that must be collected and recorded in order for the intercept to be used later as evidence in a legal proceeding. Therefore, in every type of interception there is a need to determine the presence, identity, and location of the parties of the specified communication.

A key aspect of a LI solution is the requirement that interceptions be undertaken and delivered to the requesting agencies in real-time and encapsulated in a standard format that includes appropriate labelling and meta-data that can withstand scrutiny in court. The intercepted communications must also be delivered over an encrypted channel. The encapsulation format and delivery handovers are defined in sets of standards documents issued by telecommunications governance bodies; the most common of these standards are those published by the European Telecommunications standards Institute (ETSI). Majority of the European and the Asia-Pacific countries follow ETSI requirements. ETSI is a standardization organisation in the field of information and communications. ETSI’s main goal is

to remove all deviations from global standards and to focus on a defined set of requirements while ensuring interoperability among standards.

About OpenLI

OpenLI is the world's first open-source LI software solution and provides network operators with a low-cost alternative for complying with the LI requirements in their jurisdiction. The OpenLI software has been developed by the WAND Network Research group at the University of Waikato. For more information visit our [website](#).



OpenLI
Lawful interception solution