INTERNET SERVICE PROVIDERS ASSOCIATION OF NEW ZEALAND

ISPANZ INFORMATION PAPER

LAWFUL INTERCEPTION

Introduction

Lawful interception (LI) in New Zealand is governed by the Telecommunications (Interception Capability & Security) Act 2013 (TICSA), which is available here: http://www.legislation.govt.nz/act/public/2013/0091/latest/whole.html#DLM5178024.

TICSA states that a network operator must ensure that every public telecommunications network that the operator owns, controls, or operates, and every telecommunications service that the operator provides in New Zealand, has full interception capability.

This document is intended to help ISPANZ members understand their obligations under TICSA.

Who Has to Provide 'Full Interception Capability'?

TICSA defines a network operator as either:

- a person who owns, controls, or operates a public telecommunications network; or
- a person who supplies (whether by wholesale or retail) another person with the capability to provide a telecommunications service.

The Interpretation Act 1999 states that the term 'person' includes a body corporate. A company is a form of body corporate. Your ISP is a 'person'.

TICA's definition of 'network operator' is much broader than the definition in the Telecommunications Act 2001. You do not need to have been declared a 'network operator' by notice in the *Gazette* to be covered by TICSA. ISPANZ's rules define an ISP as a company that offers IP connectivity to the commercial or residential public; that is, providing and operating IP transit between the customer location or

connection and the global Internet. Every Full Member of ISPANZ is therefore subject to TICSA. This means that every Full Member of ISPANZ must, unless they qualify for 'reduced duties', have full interception capability.

Do I Qualify for 'Reduced Duties'?

If you have less than 4,000 customers you may qualify for 'reduced duties' by providing supporting information to the registrar. 'Network operators' who qualify need only be 'intercept ready' at all times.

Infrastructure level services and wholesale network services also qualify for lower levels of compliance. You must provide customer details to the registrar for all customers to whom you provide infrastructure level services. Wholesale network services must be 'intercept accessible'.

What do The Interception Terms Mean?

Full Interception Capability is defined in TICSA Part 2, Subpart 1.

Intercept Ready and **Intercept Accessible** are defined in TICSA Part 2, Subpart 2.

For ease of reference some excerpts of TICSA's provisions (as at September 2017) are included as an appendix. Please read the complete Act to see these excerpts in context.

What Action do I Need to Take?

Register. Firstly, if you are a 'network operator' as defined by TICSA (and all ISPANZ Full Members will be) you must register. You should have registered within three months of TICSA coming into force, or within three months of becoming a 'network operator', whichever is the later. You can contact the registrar by following this link: https://forms.police.govt.nz/forms/contact-ticsa-registrar/57

Security Clearance. Unless you have less than 4,000 customers you must nominate a suitable employee for a secret-level, government-sponsored security clearance.

Provide Information. You must comply with requests for information issued in accordance with TICSA even if the information is commercially sensitive or protected by a confidentiality agreement.

Compliance Testing. You may be required to submit your equipment and procedures to compliance testing to confirm that they allow you to meet your obligations under TICSA, and to provide a certificate confirming compliance.

Assist Surveillance Agencies. You must assist surveillance agencies who have an interception warrant or any other lawful interception authority.

How Do I Recognise a Lawful Warrant or Authority?

Lawful warrants and authorities only come from three organisations:

- NZ Police.
- NZ Security Intelligence Service (NZSIS).
- Government Communications Security Bureau (GCSB).

An **NZ Police surveillance device warrant** will be provided to your authorised staff member. In some situations of emergency or urgency the NZ Police may use a surveillance device without warrant for a period not exceeding 48 hours. In these circumstances you will be contacted by an NZ Police representative.

An **NZSIS interception warrant** will be shown to the chief executive (or their delegate). It will state clearly that it is a warrant authorising interception and will be signed by the Prime Minister and, in the case of a domestic warrant, also by the Commissioner of Security Warrants. The warrant is a classified document so must not be copied and will not be left with you, though the chief executive will be provided with a certificate, signed by the Director of Security, identifying that the warrant has been served.

A **GCSB Interception Warrant or Access Authorisation** will be shown to the chief executive (or their delegate). It will state clearly what actions are being authorised and will be signed by the Minister responsible for the GCSB and, in cases that

authorise access to the private communications of New Zealanders, also by the Commissioner of Security Warrants. The Interception Warrant or Access Authorisation is a classified document so must not be copied and will not be left with you, though the chief executive will be provided with a letter, signed by the Director of GCSB, identifying that the Interception Warrant or Access Authorisation has been served.

ISPANZ **strongly recommends** that you confirm the identity of anyone presenting what appears to be one of the above documents. They should be able to produce photo ID issued by their organisation. They should also be able to provide you with a telephone number for their superior.

What About My Costs?

TICSA states; “The costs of developing, installing, and maintaining an interception capability on a public telecommunications network or a telecommunications service must be paid for by the network operator concerned.”

It also states that; “A surveillance agency must pay for the actual and reasonable costs incurred by a network operator or a service provider in providing assistance to the agency . . .”

This Looks Difficult and I Would Like Help

TICSA Clause 27 allows network operators to co-ordinate, share, or contract for services (whether equipment or staff) in order to meet the interception capability requirements in the Act.

ISPANZ is investigating ways to ease the burden on Members in complying with TICSA. As it is developed, further advice and guidance will be included in this Information Paper.

ETSI has a number of relevant publications. If you would like to do your own research, two places you might start are:

- ETSI TS 101 331 which covers the requirements of law enforcement agencies and is available here: http://www.etsi.org/deliver/etsi_ts/101300_101399/101331/01.05.01_60/ts_101331v010501p.pdf
- ETSI TS 102 232-1 which is a handover specification for IP delivery and is available here: http://www.etsi.org/deliver/etsi_ts/102200_102299/10223201/02.01.01_60/ts_10223201v020101p.pdf

Enforcement

TICSA has various enforcement provisions, including a provision for fines.

What if I Think That Some of TICSA's Provisions Should Not Apply to Me?

TICSA Part 2, Subpart 4 contains provisions for exemptions to be allowed. Such exemptions are likely to be granted sparingly. If you think that you have a special case, you should contact the registrar to discuss your situation – but don't hold your breath.

ISPANZ Associate Members

Associate members, whilst probably not being 'network operators', may be telecommunications service providers. If you are, you should be aware that the Minister may, at the application of a surveillance agency, direct that a telecommunications service provider have 'full interception capability', be 'intercept ready' or be 'intercept accessible'; and be treated as having the same obligations and rights as a 'network operator'.

Advice

ISPANZ advises all its members to read TICSA, which is available here:
http://www.legislation.govt.nz/act/public/2013/0091/latest/whole.html#DLM5178024

Other useful information is available from the NZ Police:
http://www.police.govt.nz/advice/businesses-and-organisations/ticsa

If you are in any doubt as to your responsibilities, and what it takes to comply with them, you should contact NZ Police and/or seek professional legal advice. This document is intended only as an introduction to your obligations under TICSA. It is not a complete guide to your compliance obligations.

Appendix – Excerpts from TICSA

Full Interception Capability

TICSA Part 2, Subpart 1, Clause 10(1) states:

> A public telecommunications network or a telecommunications service has full interception capability if every surveillance agency that is authorised under an interception warrant or any other lawful interception authority to intercept telecommunications or services on that network, or the network operator concerned, is able to—
>
> > (a) identify and intercept telecommunications without intercepting telecommunications that are not authorised to be intercepted under the warrant or lawful authority; and
> >
> > (b) obtain call associated data relating to telecommunications (other than telecommunications that are not authorised to be intercepted under the warrant or lawful authority); and
> >
> > (c) obtain call associated data and the content of telecommunications (other than telecommunications that are not authorised to be intercepted under the warrant or lawful authority) in a useable format; and
> >
> > (d) carry out the interception of telecommunications unobtrusively, without unduly interfering with any telecommunications, and in a manner that protects the privacy of telecommunications that are not authorised to be intercepted under the warrant or lawful authority; and
> >
> > (e) undertake the actions referred to in paragraphs (a) to (d) efficiently and effectively and,—
> >
> > > (i) if it is reasonably achievable, at the time of transmission of the telecommunication; or
> > >
> > > (ii) if it is not reasonably achievable, as close as practicable to that time.

INTERNET SERVICE PROVIDERS ASSOCIATION OF NEW ZEALAND

Intercept Ready

TICSA Part 2, Subpart 2, Clause 11(1) states:

> A network operator that is required by or under this subpart to ensure that a network or service is intercept ready—
>
> (a) must pre-deploy access points at suitable and sufficient concentration points on the network or service to allow an interception warrant or any other lawful interception authority relating to any of its customers to be given effect:
>
> (b) must reserve 1 or more network interfaces (that is, delivery ports) to which interception equipment can connect in order to deliver intercepted telecommunications to the surveillance agency; and
>
> (c) must reserve, for each reserved interface referred to in paragraph (b), sufficient bandwidth to deliver intercepted telecommunications content and call associated data to the relevant surveillance agency; and
>
> (d) when presented with an interception warrant or any other lawful interception authority must, free of charge,—
>
> (i) provide a suitable access point in its public telecommunications network or service for interception equipment:
>
> (ii) co-operate with authorised persons and allow them access to its premises:
>
> (iii) provide sufficient environmentally controlled space to house the interception equipment or provide sufficient backhaul to a suitable location where the equipment can be housed:
>
> (e) must, when compliance with the Act is required to be tested, comply with paragraphs (a) to (d).

INTERNET SERVICE PROVIDERS
ASSOCIATION OF NEW ZEALAND

Intercept Accessible

TICSA Part 2, Subpart 2, Clause 12 states:

> A network operator that is required by or under this subpart to ensure that a network or service is intercept accessible must, when presented with an interception warrant or any other lawful interception authority, be willing and able to—
>
> > (a) provide a suitable access point in its public telecommunications network or service for interception equipment:
> >
> > (b) co-operate with authorised persons and allow them access to its premises:
> >
> > (c) provide sufficient environmentally controlled space to house the interception equipment or provide sufficient backhaul to a suitable location where the equipment can be housed.