

Telecommunications (Interception Capability) Bill

Government Bill

As reported from the Law and Order Committee

Commentary

Recommendation

The Law and Order Committee has examined the Telecommunications (Interception Capability) Bill and recommends that it be passed with the amendments shown.

Background

The bill does not change or extend in any way the existing powers of surveillance agencies to intercept communications. The bill places a legislative obligation on telecommunications network operators to be technically able to intercept communications going over their network, when such interceptions are authorised by a warrant issued to the New Zealand Police, the Government Communications Security Bureau, the New Zealand Security Intelligence Service, or any other lawful authority.

This legislation is necessary to prevent law enforcement and national security capability being seriously eroded because of technical issues related to telecommunications networks. This is reflected in clause 5, the purpose clause, which states that one purpose of the bill is to ensure that surveillance agencies are able to effectively carry out the lawful interception of telecommunications.

In addition, all telecommunications network operators and service providers will be subject to a legislative 'duty to assist', to provide reasonable assistance to the surveillance agencies in executing an

interception warrant, within their technical capability and on a cost-recovery basis.

Who is a ‘network operator’, and who is a ‘service provider’?

A network operator means any person, company, or business that owns, controls, or operates a telecommunications network that can be used for public communications (for example Telecom New Zealand Limited, TelstraClear Limited and Vodafone New Zealand Limited). The person, company, or business may also be a wholesaler of the network capability to other network operators.¹

The public telecommunications network includes all telecommunications networks that can be accessed or used by the public. This includes fixed and cellular telephone networks, and the newer data networks associated with email and the Internet.

A service provider means any person, company or business that provides a public telecommunications service to an end user. The service provider role extends to all those who provide public telecommunications services, for example, owners of hotels, motels, and Internet cafés. By definition, a service provider does not include a network operator. However, a network operator may also be a service provider.

What is the ‘duty to assist’?

Clause 13 of the bill sets out the obligations on the network operator and the service provider in relation to the ‘duty to assist’. The ‘duty to assist’ requires the network operator and service provider to assist the surveillance agency to intercept communications by making available people to provide any reasonable technical assistance that may be necessary to provide interception, and taking all other reasonable steps to give effect to the interception.

What does having ‘interception capability’ mean?

The bill requires network operators to ensure that their public telecommunications networks have ‘interception capability’. Clause 8

¹ We have recommended a change to this definition to clarify that this requirement extends to wholesalers as well as retailers. The recommendation is explained under the heading ‘Definition of ‘network operator’ to be clarified’ on page 10.

of the bill spells out that, in order to be interception capable, a telecommunications network must be able to:

- identify and intercept exclusively the telecommunications authorised to be intercepted;
- obtain relevant information about call associated data and the content of communications in a usable format;
- intercept unobtrusively while protecting the privacy of other telecommunications;
- undertake the actions referred to above efficiently, effectively, and in a timely manner.

The bill is similar to recent overseas legislation

The bill is similar to legislation already in force in a number of other countries, including the United States, the United Kingdom, and Australia.

Australia—Commonwealth Telecommunications Act 1997

In Australia the relevant legislation is the Commonwealth Telecommunications Act 1997, which states, in general terms, that all carriers and carriage service providers must give the authorities such help as is reasonably necessary for purposes relating to law enforcement and national security.² Giving help includes the provision of interception services, including services in executing an interception warrant. Companies bear the capital and ongoing costs of developing, installing, and maintaining interception capability, as well as the costs of providing the information to the ‘delivery point’. The law enforcement agencies bear the costs from the ‘delivery point’ to their monitoring site, any costs associated with agency-specific capabilities, and the one-off costs of executing each warrant.

United Kingdom—Regulation of Investigatory Powers Act 2000

In the United Kingdom, the Regulation of Investigatory Powers Act 2000 provides for a power allowing the Secretary of State to impose obligations upon communication service providers to maintain a

² A carrier is the holder of a carrier licence and the obligation to have a carrier licence arises from the ownership or control of a network. A carriage service provider supplies or proposes to supply a listed carriage service to the public using a network unit.

reasonable interception capability.³ The obligations that the Secretary of State considers reasonable to impose are set out in an order.⁴ The order does not impose specific requirements on providers, but describes in general terms the kind of intercept capability required. To impose the obligations in the order, the Secretary of State may serve a notice on a communication service provider setting out the steps it must take to ensure that the obligations are met. If a communication service provider is served with a notice and considers the technical or financial consequences of complying to be unreasonable, the provider may refer the notice to the Technical Advisory Board, which is made up of experts from the Government and industry. The Technical Advisory Board advises the Home Secretary of its view of reasonableness, and the Home Secretary may withdraw, confirm, or modify the notice.

Submissions received on the bill

We received submissions from telecommunications companies, as well as from the Police Association and concerned members of the public. The Police Association supported the bill, believing it will help reduce the influence of serious organised crime and enhance the ability of the Police to investigate crime. The telecommunications companies supported the aims of the bill, seeing the value of surveillance agencies gaining interception capability and the need for this capability to keep pace with technological developments. However, they believed that some aspects of the bill needed to be changed. This included a dispute over the original estimated cost of compliance. We believe the amendments we have recommended address their concerns.

Of the four individuals or groups of concerned members of the public who made submissions, three were opposed to the bill, thinking it was an overreaction to the terrorist events of 11 September 2001, and an intrusion into personal privacy.

³ Communication service providers are those providers who provide publicly available communications services including postal, telecommunications, and Internet companies.

⁴ Regulation of Investigatory Powers (Maintenance of Interception Capability) Order 2000.

A phased implementation process is included in the bill

A phased implementation process is included in the bill in order to provide the industry with an opportunity to implement the necessary technical changes in a way that is cost efficient.

Network operators of fixed and mobile voice networks have an 18-month period from when the bill is passed in which to attain interception capability. Network operators of Internet and email services have a five-year period from when the bill is passed in which to attain interception capability.

The dates for implementation in clauses 15(1)(a) and 15(1)(b) in the original bill have to be amended from the specific dates set down, as these specific dates will not allow for the 18-month and five-year time periods for network operators to gain interception capability from when the bill is passed.

Cost of compliance for telecommunications companies

The Government will pay all costs related to the provision of interception capability for fixed and mobile voice networks that were operational on 12 November 2002.⁵ Those network operators providing fixed or mobile voice networks that were not operational on 12 November 2002 will need to meet their own costs in the provision of interception capability. Network operators will need to meet their own costs of providing for interception capability for Internet and email services.

Original estimated costs to telecommunications companies

In the explanatory note to the bill, compliance costs to be borne by the telecommunications companies were estimated to be \$12 million. This figure was ascertained after consultation with the affected companies during the drafting of the bill.

Telecommunications companies disputed the original estimated costs

During our consideration of the bill, the Telecommunications Carriers' Forum and Telecom New Zealand Limited submitted additional information on the costs at variance with the information obtained in

⁵ This is the date on which the bill was introduced to the House.

the development stage of the bill.⁶ The Telecommunications Carriers' Forum provided two figures: the first, which assumed the use of probes in a network, was \$23.576 million, while a larger figure of more than \$43.576 million was based on all network elements having an interception capability. The bill, however, does not require this, and this issue is canvassed more fully under the heading 'Interception capability does not need to be installed on each element of the network' on page seven.

Further discussions with telecommunications companies confirmed the original estimated costs

Given that the telecommunications companies disputed the estimated costs that would be borne by them to ensure they were 'interception capable', further consultation was undertaken with some members of the Telecommunications Carriers' Forum, along with Telecom New Zealand Limited and Broadcast Communications Limited, to establish why there was a difference in the figures from \$12 million in the development stage of the bill to the \$23.576 million claimed in its submission.⁷

After these discussions and the revision of figures, the cost estimate for the delivery of data interception capability is now in the range of \$10.2 to \$13.4 million, making the estimate of \$12 million determined in the development stages appropriate.

Costs incurred in assisting surveillance agencies

Under clause 18, surveillance agencies are required to pay the actual and reasonable costs incurred by a network operator or service provider giving assistance under the duty to assist clause. We recommend that surveillance agencies have only one month in which to pay an invoice rather than two months. This will lessen the cash flow burden on operators assisting surveillance agencies.

⁶ The Telecommunications Carriers' Forum was formed under the Telecommunications Act 2001. Its purpose is to facilitate co-operation amongst telecommunications carriers to encourage the efficient provision of both regulated and non-regulated telecommunications services. The current members are Telecom New Zealand Limited, TelstraClear Limited, Vodafone New Zealand Limited, CallPlus New Zealand Limited, The Internet Group Limited (Ihug), WorldxChange Communications Limited, Broadcast Communications Limited, and CityLink.

⁷ Even though Broadcast Communications Limited and Telecom are part of the Telecommunications Carriers' Forum, they also made separate submissions on the bill. They were therefore consulted separately at this stage.

Amendments related to interception duties and the position of the intercepted communication

Interception capability does not need to be installed on each element of the network

The intent of the bill is to ensure that all public telecommunications are able to be intercepted, and that the network operators provide the interception capability in the manner that best suits their network. In modern digital telecommunications networks, the interception of non-voice telecommunications can be carried out either by having an in-built interception capability in every network element, or by using external (or mobile) probes at selected locations throughout a network. Having interception capabilities built into every network element is very expensive and is considered unnecessary. Instead, the bill allows for the use of probes, thus providing the network operators with much greater flexibility at a much lower cost.

We recommend that clause 7 be amended to ensure it is clear that interception capability does not need to be installed within each element of the telecommunications network or telecommunications service. The Telecommunications Carriers' Forum and Telecom New Zealand Limited perceived this clause to mean that each network and service was required to have interception capability installed within it, rather than providers having the freedom to choose their own design features and specifications as appropriate, which is what clause 5(c) intends. This change will clarify that network operators and service providers have the freedom to choose where and how they provide the interception capability within the network elements.

Network operators may be required to carry out an interception

Clause 8 requires a surveillance agency to carry out the interception. The Telecommunications Carriers' Forum and Telecom New Zealand Limited pointed out that, in practice, network operators or their agents, not the surveillance agency, will carry out the interception in many cases. We recommend an amendment to clarify that in some cases the network operator will carry out the interception.

Interception to be completed when the information is delivered to the agency

We recommend an amendment to clause 8, as we consider that the requirement to intercept should be completed when the information is passed onto the surveillance agency. This provision is lacking in the current bill. The amendment sets out that the network operator needs to be able to deliver intercepted telecommunications and call associated data to the surveillance agency. Details as to the location will need to be decided by the network operator in consultation with the surveillance agency. Any telecommunications links required between the delivery point and the surveillance agencies can be provided by any network operator at normal commercial rates. Delivery will need to be effected over appropriately encrypted links as required to meet the security requirements of the surveillance agencies.

Limitations placed on the requirement to decrypt

We recommend that limitations should also be placed on the requirement to decrypt in clause 8. Our view is that there should be a requirement on network operators to decrypt telecommunications that they already have the key to decrypt. However, it may not be fair or reasonable to expect a network operator to provide decryption for services it has on-sold to a customer. This may place the network operator at a commercial disadvantage. It would not be able to sell a particular product if it did not have a key to decrypt it, but a customer could buy exactly the same product from a retail outlet and then use it over the operator's network. This should be distinguished from a situation where a network operator has its own encryption facility or contracts a manufacturer to provide an encryption facility. In these situations we consider that a network operator should be required to provide decryption.

Concerns about terms and definitions in the interpretation clause**The term 'call associated data' to remain the same**

Telecom New Zealand Limited recommended changing the term 'call associated data' to 'telecommunications associated data'. We do not recommend this change. Although 'telecommunications associated data' may be more appropriate, it is important to maintain

consistency with other legislation (for example, the Telecommunications (Residual Provisions) Act 1987). We note that the first line of the definition clarifies that it relates to all telecommunications, not just calls.

Definition of ‘network operator’ to be clarified

We recommend clarifying the definition of the term ‘network operator’, to make it clear that all network operators providing either retail or wholesale network capacity are required to provide interception capabilities, that is, the requirement extends to those who supply wholesale or retail capability to any other person to provide public telecommunications.

Definition of ‘number’ to be changed

We recommend that the definition of the term ‘number’ be changed to encompass addresses and identifiers other than those specifically for analogue telephone calls. This amendment expands the list of what is considered a ‘number’ to include a unique identifier for a telecommunication (for example, an electronic serial number), and a user account identifier, and for accuracy replaces the term ‘Internet address’ with ‘Internet Protocol address’.

Definition of ‘public data network’ to be clarified

We recommend changes to the definition of ‘public data network’ to ensure that it is clear what this term means, by changing the terms ‘Internet’ and ‘email’ already included in the definition to ‘Internet access’ and ‘email access’. This amendment ensures that the bill covers the network-provided capabilities and access to and from the services only, not the services themselves.

Amendments made to the regulation-making powers in the bill

The Regulations Review Committee reported to us on the regulation-making powers contained in clause 28 of the bill. That committee was concerned about:

- the generality of the regulation-making powers in clauses 28(1)(a) and 28(1)(c);

- the qualification in 28(4), as it limits the possibility of judicial intervention if the Minister fails to have regard to the criteria and consultation requirements in 28(2).

We agree that these concerns are legitimate and that amendments need to be made to the bill to address them. As such, we recommend that clause 28(1)(a) be deleted, as it is too general. We consider that matters surrounding the timing of interception are adequately covered by clause 8.

In addition, we recommend that clause 28(1)(c) be deleted. As currently worded it is a general regulation-making power. Originally we had wanted to include some parameters or requirements to more clearly define the concept of ‘minimum interference’, otherwise there was a danger that the regulations would have been able to determine how an interception was carried out. However, we had difficulty defining the parameters around ‘minimum interference’ in a meaningful way. We consider that the requirements for privacy are already protected in the legislation, through clauses 6, 8 and 14.

We recommend that a general regulation-making power be included in the bill, providing for any other matters that are necessary for the bill’s administration, and necessary for giving it full effect.

We note the Regulations Review Committee’s concern about clause 28(4). The committee stated that the provision limits the possibility of judicial intervention if the Minister fails to have regard to the criteria and consultation requirements in clause 28(2), and recommended that we consider deleting this clause.

We agree and recommend that clause 28(4) be deleted. Further consideration of the regulation-making power and amendments to it have led to the conclusion that this clause is redundant. Clause 28(3) gives the Minister the power to dispense with the requirements in clause 28(2), if the Minister considers it desirable in the public interest that the Order in Council be made urgently. In all other cases we would envisage that the requirements would be met.

Appendix

Committee process

The Telecommunications (Interception Capability) Bill was introduced to the House on 12 November 2002 and referred to the Law and Order Committee on 18 February 2003. The closing date for submissions was 9 April 2003. We received and considered nine submissions from interested groups and individuals, of which we heard five. Total consideration took 6 hours and 21 minutes, of which hearings of evidence took 1 hour and 48 minutes.

We received advice from the Ministry of Justice and the New Zealand Police. The Regulations Review Committee reported to the committee on the powers contained in clause 28.

Committee membership

Martin Gallagher (Chairperson)

Marc Alexander (Deputy Chairperson)

Georgina Beyer

Brian Connell

Ann Hartley

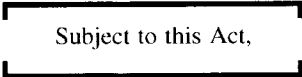
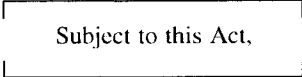
Mahara Okeroa

Edwin Perry

Hon Tony Ryall

Key to symbols used in reprinted bill

As reported from a select committee

Struck out (unanimous)	
	Text struck out unanimously
New (unanimous)	
	Text inserted unanimously
<i>(Subject to this Act.)</i>	Words struck out unanimously
<u>Subject to this Act,</u>	Words inserted unanimously

Hon Lianne Dalziel

Telecommunications (Interception Capability) Bill

Government Bill

Contents

1	Title	
	Part 1	
	Preliminary provisions	
	<i>General</i>	
2	Commencement	
3	Interpretation	
4	Act binds the Crown	
	<i>Purpose and principles</i>	
5	Purpose	
6	Principles	
	Part 2	
	Interception duties	
	<i>Duty to have interception capability</i>	
7	Network operators must ensure public telecommunications networks and telecommunications services have interception capability	
8	When duty to have interception capability is complied with	
	<i>Limits on duty to have interception capability</i>	
9	Certain facilities excluded from scope of duty under section 7	
10	Design of networks not affected by this Act	
	<i>Exemptions</i>	
11	Minister may grant exemptions	
12	Minister must consult responsible Ministers before granting exemption	
	<i>Duty to assist</i>	
13	Duty to assist surveillance agencies	
14	Duty to minimise impact of interception on third parties	
	Part 3	
	Miscellaneous provisions	
	<i>Transitional provision</i>	
15	Network operators have lead-in time to attain interception capability	
	<i>Allocation of costs relating to interception capability</i>	
16	Allocation of costs of interception capability on public switched telephone network or telecommunications service	
17	Costs of interception capability on public data network	
	<i>Costs relating to interceptions</i>	
18	Costs incurred in assisting surveillance agencies	
	<i>Resolution of disputes about costs</i>	
19	Dispute about costs must be referred to mediation or arbitration	
	<i>Protection from liability</i>	
20	Protection from liability	
	<i>Compliance orders</i>	
21	Power of High Court to order compliance	
22	Application for compliance order	
23	Right to be heard	
24	Decision on application	
	<i>Appeals against making of compliance order</i>	
25	Appeals to Court of Appeal	
26	Effect of appeal	
	<i>Enforcement</i>	
27	Pecuniary penalty for contravention of compliance order	
	<i>Regulations</i>	
28	Regulations	

The Parliament of New Zealand enacts as follows:**1 Title**

This Act is the Telecommunications (Interception Capability) Act 2002.

Part 1
Preliminary provisions

5

General

2 Commencement

This Act comes into force on the day after the date on which it receives the Royal assent.

10

3 Interpretation

(1) In this Act, unless the context otherwise requires,—

call associated data, in relation to a telecommunication,—

(a) means information—

- (i) that is generated as a result of the making of the telecommunication (whether or not the telecommunication is sent or received successfully); and
- (ii) that identifies the origin, direction, destination, or termination of the telecommunication; and

15

(b) includes, without limitation, any of the following information:

20

- (i) the number from which the telecommunication originates;
- (ii) the number to which the telecommunication is sent;
- (iii) if the telecommunication is diverted from one number to another number, those numbers;
- (iv) the time at which the telecommunication is sent;
- (v) the duration of the telecommunication;
- (vi) if the telecommunication is generated from a mobile telephone, the point at which the telecommunication first enters a network; but

25

(c) does not include the content of the telecommunication
compliance order means an order made by the High Court under **section 21**

30

35

end-user, in relation to a telecommunications service, means a person who is the ultimate recipient of that service or of another service the provision of which is dependent on that service

intelligence and security agency means—

- (a) the New Zealand Security Intelligence Service; or
- (b) the Government Communications Security Bureau

intercept, in relation to a private telecommunication, (*means*) includes hear, listen to, record, monitor, acquire, or receive the telecommunication either—

- (a) while it is taking place on a telecommunications network; or
- (b) while it is in transit on a telecommunications network

interception capability means the capability to intercept a telecommunication as described in **section 8**

interception warrant means a warrant that is issued to a surveillance agency under any of the following enactments:

- (a) section 312C or section 312CB or section 312G of the Crimes Act 1961;
- (b) section 4A(1) or (2) of the New Zealand Security Intelligence Service Act 1969;
- (c) section 15 or section 15B or section 19 of the Misuse of Drugs Amendment Act 1978:

Struck out (unanimous)

- (d) section 17 of the Government Communications Security Bureau Act **2001**

New (unanimous)

- (d) section 17 of the Government Communications Security Bureau Act 2003

law enforcement agency means—

- (a) the New Zealand Police; or
- (b) any government department declared by the Governor-General, by Order in Council, to be a law enforcement agency for the purposes of this Act

Minister means the Minister of the Crown who, under the authority of any warrant or with the authority of the Prime Minister, is for the time being responsible for the administration of this Act

Struck out (unanimous)

network operator means any person who owns, controls, or operates a public telecommunications network 5

New (unanimous)

network operator means—

- (a) a person who owns, controls, or operates a public telecommunications network; or
- (b) a person who supplies (whether by wholesale or retail) another person with the capability to provide a telecommunications service 10

Struck out (unanimous)

number—

- (a) means the address used for the purposes of a telecommunication; and 15
- (b) includes any of the following:
 - (i) a telephone number;
 - (ii) a mobile telephone number;
 - (iii) an Internet address;
 - (iv) an email address 20

New (unanimous)

number—

- (a) means the address used by a network operator or a telecommunications service for the purposes of—
 - (i) directing a telecommunication to its intended destination; and 25

New (unanimous)

- (ii) identifying the origin of a telecommunication;
and
- (b) includes, without limitation, any of the following:
 - (i) a telephone number:
 - (ii) a mobile telephone number: 5
 - (iii) a unique identifier for a telecommunication device (for example, an electronic serial number or a Media Access Control address):
 - (iv) a user account identifier:
 - (v) an Internet Protocol address: 10
 - (vi) an email address

other lawful interception authority means an authority—

- (a) to intercept a private communication that is granted to any member of the New Zealand Police under section 216B(3) of the Crimes Act 1961; or 15

Struck out (unanimous)

- (b) to access a computer system of a specified foreign organisation or a foreign person (within the meaning of the Government Communications Security Bureau Act 2001) that is granted under section 20 of that Act

New (unanimous)

- (b) to access a computer system of a specified foreign organisation or a foreign person (within the meaning of the Government Communications Security Bureau Act 2003) that is granted under section 19 of that Act 20

public data network—

- (a) means a data network used, or intended for use, in whole or in part, by the public; and 25
- (b) includes, without limitation, the following facilities:

Struck out (unanimous)

- (i) the Internet;
- (ii) email

New (unanimous)

- (i) Internet access; and
- (ii) email access

- public switched telephone network** means a dial-up telephone network used, or intended for use, in whole or in part, by the public for the purposes of providing telecommunication between telecommunication devices 5
- public telecommunications network** means—
- (a) a public switched telephone network; and 10
 - (b) a public data network
- responsible Ministers** means—
- (a) the Minister in charge of the New Zealand Security Intelligence Service; and
 - (b) the Minister in charge of the Government Communications Security Bureau; and 15
 - (c) the Minister of Police
- service provider**—
- (a) means any person who provides a telecommunications service to an end-user (whether or not as part of a business undertaking and regardless of the nature of that business undertaking); but 20
 - (b) does not include a network operator
- surveillance agency** means—
- (a) a law enforcement agency; or 25
 - (b) an intelligence and security agency
- telecommunication device**—
- (a) means any terminal device capable of being used for transmitting or receiving a telecommunication over a network; and 30
 - (b) includes a telephone device.

- (2) In this Act, unless the context otherwise requires, **network**, **telecommunication**, **telecommunication link**, **telecommunications service**, and **telephone device** have the meanings given to them by section 5 of the Telecommunications Act 2001. 5
- 4 Act binds the Crown**
This Act binds the Crown.
- Purpose and principles*
- 5 Purpose** 10
The purpose of this Act is to ensure—
- (a) that surveillance agencies are able to effectively carry out the lawful interception of telecommunications under an interception warrant or any other lawful interception authority; and
 - (b) that surveillance agencies, in obtaining assistance for the interception of telecommunications, do not create barriers to the introduction of new or innovative telecommunications technologies; and 15
 - (c) that network operators and service providers have the freedom to choose system design features and specifications that are appropriate for their own purposes. 20
- 6 Principles**
The following principles must be applied by persons who exercise powers and carry out duties under this Act if those principles are relevant to those powers or duties: 25
- (a) the principle that the privacy of telecommunications that are not subject to an interception warrant or any other lawful interception authority must be maintained to the extent provided for in law:
 - (b) the principle that the interception of telecommunications, when authorised under an interception warrant or any other lawful interception authority, must be carried out without unduly interfering with any telecommunications. 30

Part 2 Interception duties

Duty to have interception capability

- 7 Network operators must ensure public telecommunications networks and telecommunications services have interception capability** 5
- (1) 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 an interception capability. 10
- New (unanimous)**
- (1A) However, **subsection (1)**—

(a) does not require a network operator to ensure that all components of the public telecommunications network or telecommunications service referred to in that subsection have an interception capability; and 15

(b) is sufficiently complied with if a network operator ensures, in whatever manner the network operator thinks fit, that at least 1 component of that network or service has an interception capability.
- (2) Without limiting **subsection (1)**, the duty under that subsection to have an interception capability includes the duty to ensure that the interception capability is developed, installed, and maintained. 20
- 8 When duty to have interception capability is complied with** 25
- (1) A public telecommunications network or a telecommunications service has an 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 service), or the network operator concerned, is able to— 30
- (a) identify and intercept telecommunications without intercepting telecommunications that are not authorised to be intercepted under the warrant or authority; and
- (b) obtain call associated data relating to telecommunications (other than telecommunications that are not 35

- authorised to be intercepted under the warrant or 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 authority) in a format that is able to be used by the agency; and 5
 - (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 authority; and 10
 - (e) undertake the actions referred to in **paragraphs (a) to (d)** efficiently and effectively and,— 15
 - (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.

New (unanimous)

- (1A) If a network operator, or an employee or agent of a network operator, undertakes the interception of a telecommunication on behalf of a surveillance agency under **subsection (1)**, the interception must be taken to be complete when the network operator provides the call associated data or the content of the telecommunication, or both, to the surveillance agency. 20
- (2) A network operator must, in order to comply with **subsection (1)(c)**, decrypt a telecommunication on that operator's public telecommunications network or telecommunications service if— 25
- (a) the content of that telecommunication has been encrypted; and 30
 - (b) the network operator intercepting the telecommunication has provided that encryption.

Struck out (unanimous)

- (3) Nothing in this section requires a network operator to ensure that a surveillance agency has the ability to decrypt any telecommunication.

New (unanimous)

- (3) However, **subsection (2)** does not require a network operator to— 5
- (a) decrypt any telecommunication on that operator's public telecommunications network or telecommunications service if the encryption has been provided by means of a product that is— 10
- (i) supplied by a person other than the operator and is available on retail sale to the public; or
- (ii) supplied by the operator as an agent for that product; and
- (b) ensure that a surveillance agency has the ability to decrypt any telecommunication. 15

*Limits on duty to have interception capability***9 Certain facilities excluded from scope of duty under section 7****Struck out (unanimous)**

Despite **section 7**, a network operator is not required to have an interception capability for facilities used for interconnection between public telecommunications networks. 20

New (unanimous)

Despite **section (7)**, a network operator is not required to have an interception capability on a telecommunication link that is used to interconnect 2 or more public telecommunications networks. 25

10 Design of networks not affected by this Act

This Act does not authorise a surveillance agency to—

- (a) require any person to adopt a specific design or feature for any network; or
- (b) prohibit any person from adopting any specific design or feature for any network. 5

Exemptions

11 Minister may grant exemptions

- (1) The Minister may exempt any network operator from the requirements of **section 7** or from the requirements of all or any of the provisions of **section 8** (except **section 8(1)(a) and (d)**) if the Minister considers that there are special circumstances (for example, a pilot trial of a new network or telecommunications service) that justify granting an exemption. 10
- (2) The Minister may grant the exemption— 15
 - (a) unconditionally; or
 - (b) subject to any conditions the Minister thinks fit.
- (3) The exemption—
 - (a) must be granted for a period of time that the Minister specifies; and 20
 - (b) may, at any time, be varied or revoked by the Minister.

12 Minister must consult responsible Ministers before granting exemption

- (1) Before granting, varying, or revoking an exemption under **section 11**, the Minister must consult with the responsible Ministers. 25
- (2) A failure to comply with **subsection (1)** does not affect the validity of any exemption granted under **section 11**.

Duty to assist

13 Duty to assist surveillance agencies 30

- (1) A surveillance agency to whom an interception warrant is issued, or any other lawful interception authority is granted, may, for the purpose of requiring assistance in the execution of the warrant or the authority, show to either or both of the persons referred to in **subsection (2)**,— 35

- (a) in the case of an interception warrant issued to an intelligence and security agency, a copy of the relevant parts of the warrant; or
- (b) in any other case, a copy of the warrant or evidence of the authority. 5
- (2) The persons are—
- (a) a network operator;
- (b) a service provider.
- (3) A person who is shown under **subsection (1)** a copy of an interception warrant or the relevant parts of the warrant, or evidence of any other lawful interception authority, must assist the surveillance agency by— 10
- (a) making available any of the person’s officers, employees, or agents who are able to provide any reasonable technical assistance that may be (*reasonably*) necessary for the agency to intercept a telecommunication that is subject to the warrant or authority; and 15
- (b) taking all other reasonable steps that are (*reasonably*) necessary for the purpose of giving effect to the warrant or authority. 20

New (unanimous)

- (4) For the purposes of this section, a network operator may intercept a telecommunication on behalf of a surveillance agency.

- 14 Duty to minimise impact of interception on third parties** 25
- Every person who, under an interception warrant or any other lawful interception authority, intercepts or assists in the interception of a telecommunication must take all practicable steps that are reasonable in the circumstances to minimise the likelihood of intercepting telecommunications that are not authorised to be intercepted under the warrant or authority. 30

Part 3
Miscellaneous provisions

Transitional provision

- 15 Network operators have lead-in time to attain interception capability** 5

Struck out (unanimous)

- (1) Nothing in **section 7** requires a network operator to have an interception capability on any public telecommunications network that the operator owns, controls, or operates, or any telecommunications service that the operator provides, at any time before the expiry of the period beginning on the date of commencement of this Act and ending,— 10
- (a) in the case of a public switched telephone network or a telecommunications service, on 1 October 2004; and
- (b) in the case of a public data network, on 1 April 2008.

New (unanimous)

- (1) **Section 7** does not require a network operator to have an interception capability on any public telecommunications network that the operator owns, controls, or operates, or any telecommunications service that the operator provides, at any time before the expiry of the period beginning on the date of commencement of this Act and ending,— 15
- (a) in the case of a public switched telephone network or a telecommunications service, 18 months after that commencement; and 20
- (b) in the case of a public data network, 5 years after that commencement. 25
- (2) However, any interception capability on a public telecommunications network or a telecommunications service that was in place, or that was the subject of an agreement between the Crown and a network operator, before the commencement of this Act must be developed, installed, and maintained as if **subsection (1)** and **sections 16 and 17** had not been enacted. 30

Allocation of costs relating to interception capability

- 16 Allocation of costs of interception capability on public switched telephone network or telecommunications service**
- (1) The costs incurred, during the period referred to in **section 15(1)(a)**, in ensuring that a public switched telephone network, or a telecommunications service, has an interception capability must be paid for,—
- (a) in the case of a public switched telephone network or a telecommunications service that was operational on or before the specified date, by the Crown; or
- (b) in the case of a public switched telephone network or a telecommunications service that became operational after the specified date, by the network operator that, as the case may be, owns, controls, or operates that network or provides that service.
- (2) On the expiry of the period referred to in **section 15(1)(a)**, the costs of developing, installing, and maintaining an interception capability on a public switched telephone network or a telecommunications service must be paid for by the network operator concerned.
- (3) The obligation of the Crown to pay for the costs under **subsection (1)(a)**—
- (a) relates only to the fair and reasonable costs associated with any modifications to a public switched telephone network or a telecommunications service that are necessary for that network or service to attain an interception capability; and
- (b) does not apply to the costs of upgrading a public switched telephone network or a telecommunications service that was operational on or before the specified date unless the sole purpose of upgrading that network or service is to ensure that it has an interception capability (in which case the obligation of the Crown is limited to paying for the costs connected with attaining an interception capability on that network or service and does not extend to the other costs of the upgrade).
- (4) In this section, **specified date** means the date on which this Act was introduced as a Bill into the House of Representatives.

- 17 Costs of interception capability on public data network**
The costs incurred in ensuring that a public data network has an interception capability must be paid for by the network operator that owns, controls, or operates that network.

Costs relating to interceptions 5

- 18 Costs incurred in assisting surveillance agencies**
- (1) 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 under **section 13**.
- (2) A surveillance agency must pay the costs referred to in **subsection (1)** by the date specified for payment, whether in an invoice or other appropriate document given to the agency by a network operator or a service provider, being a date not less than *(2 months) 1 month* after the date of the invoice or other appropriate document. 15

Resolution of disputes about costs

- 19 Dispute about costs must be referred to mediation or arbitration**
- (1) This section applies to any dispute about the reasonableness of the costs that are incurred, or claimed to have been incurred, in the performance of the duties imposed by this Act that arises between,— 20
- (a) in the case of costs under **sections 16 and 17**, the Crown and a network operator; or
- (b) in the case of costs under **section 13**, a surveillance agency and a network operator or a service provider. 25
- (2) If a dispute to which this section applies is unable to be resolved by agreement between the parties, the dispute must be referred to— 30
- (a) mediation; or
- (b) if the parties are unable to resolve the dispute at mediation, arbitration.
- (3) If a dispute is referred to arbitration under **subsection (2)(b)**, the provisions of the Arbitration Act 1996 apply to that dispute.

*Protection from liability***20 Protection from liability**

- (1) This section applies to—
- (a) every network operator; and
 - (b) every service provider; and 5
 - (c) every surveillance agency; and
 - (d) every person employed or engaged by a person referred to in **paragraphs (a) to (c)**.
- (2) No person to whom this section applies is liable for an act done or omitted to be done in good faith in the performance of a duty imposed, or the exercise of a function or power conferred, by this Act. 10

*Compliance orders***21 Power of High Court to order compliance**

- (1) If any person has not complied with any of the duties set out in **Part 2**, the High Court may, for the purpose of preventing any further non-compliance with those duties, make a compliance order requiring that person— 15
- (a) to do any specified thing; or
 - (b) to cease any specified activity. 20
- (2) A compliance order may be made on the terms and conditions that the High Court thinks fit, including the provision of security or the entry into a bond for performance.

22 Application for compliance order

Any officer or employee of a surveillance agency may apply to a High Court for a compliance order. 25

23 Right to be heard

Before deciding an application for a compliance order, the High Court must—

- (a) hear the applicant; and 30
- (b) hear any person against whom the order is sought who wishes to be heard.

24 Decision on application

After considering an application for a compliance order, the High Court may— 35

- (a) make a compliance order under **section 21**; or
- (b) refuse the application.

Appeals against making of compliance order

25 Appeals to Court of Appeal

- (1) A party to proceedings relating to an application for a compliance order or any other person prejudicially affected may, with the leave of the Court of Appeal, appeal to that court if the High Court—
 - (a) has made or refused to make a compliance order; or
 - (b) has otherwise finally determined or has dismissed the proceedings. 10
- (2) On an appeal to the Court of Appeal under this section, the Court of Appeal has the same power to adjudicate on the proceedings as the High Court had.
- (3) The decision of the Court of Appeal on an appeal under this section, and on an application to it under this section for leave to appeal, is final. 15

26 Effect of appeal

- Except where the Court of Appeal otherwise directs,—
- (a) the operation of a compliance order is not suspended by an appeal under **section 25**; and 20
 - (b) every compliance order may be enforced in the same manner and in all respects as if that appeal were not pending.

Enforcement 25

27 Pecuniary penalty for contravention of compliance order

- (1) If the High Court is satisfied, on the application of a surveillance agency, that a person has acted in contravention of a compliance order, the Court may order the person to pay to the Crown any pecuniary penalty that the Court determines to be appropriate. 30
- (2) The amount of any pecuniary penalty under **subsection (1)** must not exceed \$500,000.
- (3) In the case of a continuing contravention of a compliance order, the Court may, in addition to any pecuniary penalty ordered to be paid under **subsection (1)**, impose a further penalty 35

of \$50,000 for each day or part of a day during which the contravention continues.

- (4) The standard of proof in any proceedings under this section is the standard of proof that applies in civil proceedings.
- (5) Proceedings under this section may be commenced within 3 years after the matter giving rise to the contravention was discovered or ought reasonably to have been discovered. 5

Regulations

Struck out (unanimous)

- | | | |
|-----------|--|----|
| 28 | Regulations | |
| (1) | The Governor-General may, by Order in Council, make regulations for all or any of the following purposes: | 10 |
| | (a) prescribing the circumstances in which a telecommunication may be identified and intercepted at the time of transmission and the circumstances in which call associated data may be obtained at the time of transmission for the purposes of section 8(1)(a) or (b) : | 15 |
| | (b) prescribing the format in which call associated data and the content of a telecommunication must be provided for the purposes of section 8(1)(c) : | |
| | (c) prescribing the manner in which interception must be carried out to ensure that there is minimum interference to telecommunications and the privacy of telecommunications is protected for the purposes of section 8(1)(d) . | 20 |
| (2) | Before recommending the making of an Order in Council under subsection (1) , the Minister must— | 25 |
| | (a) have regard to all of the following matters: | |
| | (i) the reasonableness of making the regulations; and | |
| | (ii) the costs to network operators; and | |
| | (iii) the benefits to law enforcement and the security of the state; and | 30 |
| | (b) in relation to regulations made under subsection (1)(c) , consult with the Privacy Commissioner appointed under the Privacy Act 1993. | |

Struck out (unanimous)

- (3) **Subsection (2)** does not apply to an Order in Council if the Minister considers it desirable in the public interest that the Order in Council be made urgently.
- (4) A failure to comply with **subsection (2)** does not affect the validity of any Order in Council made under this section.

5

New (unanimous)

28 Regulations

- (1) The Governor-General may, by Order in Council, make regulations for either or both of the following purposes:
- (a) prescribing the format in which call associated data and the content of a telecommunication must be provided for the purposes of **section 8(1)(c)**; 10
 - (b) providing for any other matters contemplated by this Act, necessary for its administration, or necessary for giving it full effect.
- (2) Before recommending the making of an Order in Council under **subsection (1)(a)**, the Minister must have regard to all of the following matters: 15
- (a) the reasonableness of making the regulations; and
 - (b) the costs to network operators; and
 - (c) the benefits to law enforcement and the security of the state. 20
- (3) **Subsection (2)** does not apply to an Order in Council if the Minister considers it desirable in the public interest that the Order in Council be made urgently.

Legislative history

5 November 2002
18 February 2003

Introduction (Bill 15-1)
First reading and referral to Law and Order Committee