Telecommunications (Interception Capability) Bill

2002, No. 15--1

Government Bill

Explanatory Note

General policy statement

This Bill ensures that law enforcement and national security capability are not seriously eroded by changes in technology.

The Bill places a legislative obligation on telecommunication network operators to be technically able, if required under an interception warrant or any other lawful interception authority, to--

- intercept telecommunications; and
- investigate serious offences; and
- help protect national security.

The Bill does not change or extend in any way the existing powers of the New Zealand Police, the New Zealand Security Intelligence Service, and the Government Communications Security Bureau (the "**surveillance agencies**") to intercept telecommunications.

The provision of interception capability means that telecommunications network operators will be required to have the ability to--

- exclusively isolate and intercept telecommunications as authorised; and
- obtain relevant information about telecommunications; and
- intercept telecommunications unobtrusively while protecting the privacy of other telecommunications; and
- obtain information in a usable format.

In addition, there will be a legislative "duty to assist" on all telecommunications service providers to provide reasonable assistance to the surveillance agencies in executing an interception warrant, within their technical capability and on a cost-recovery basis.

There are a number of privacy protections included in the Bill. First, any interception is only able to be made in accordance with a lawful authorisation. Secondly, the interception capability requirements specifically refer to privacy - they include the ability to exclude telecommunications that are not authorised to be intercepted. Thirdly, telecommunications network operators are not required to decrypt any telecommunication encrypted by a customer, unless the operator provided the encryption facility.

In the interests of practicality and costs, a phased implementation process is included. The Government will pay for the provision of interception capability for existing fixed and mobile voice networks (with an 18 month implementation period). Telecommunications network operators will need to meet the costs of upgrading to provide for the interception of Internet and email services (with a 5 year implementation period) and for new or additional services (with an 18 month implementation period). It is anticipated that the 5 year implementation period should help reduce the impact on industry, as some equipment will need replacing in this time. It is easier and usually cheaper to install interception capability at the time of design and implementation of new networks than to upgrade existing networks.

Clause by clause analysis

Clause 1 is the Title clause.

Part 1

Preliminary provisions

General

Clause 2 provides that the Bill is to come into force on the day after the date on which it receives the Royal assent.

Clause 3 defines certain terms used in the Bill.

Clause 4 provides that the Bill binds the Crown.

Purpose and principles

Clause 5 is the purpose clause. The purpose of the Bill is to ensure--

- 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
- 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
- that network operators and service providers have the freedom to choose system design features and specifications that are appropriate for their own purposes.

Clause 6 sets out the principles that must be applied by persons who exercise powers and carry out duties under the Bill if those principles are relevant to those powers and duties.

Part 2

Interception duties

Duty to have interception capability

Clause 7 imposes a duty on a network operator to 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.

Clause 8 sets out the requirements for interception capability.

Limits on duty to have interception capability

Clause 9 provides that facilities used for interconnection between public telecommunications networks are not required to have an interception capability.

Clause 10 provides that the Bill does not authorise a surveillance agency to require any person to adopt, or to prohibit any person from adopting, any specific design or feature for any network.

Exemptions

Clause 11 gives the Minister the power to exempt any network operator from compliance with the duty to have an interception capability.

Clause 12 provides that, before granting, varying, or revoking an exemption under *clause 11*, the Minister must consult with the Minister in charge of the New Zealand Security Intelligence Service and the Government Communications Security Bureau and the Minister of Police.

Duty to assist

Clause 13 imposes a duty on a network operator or a service provider who is shown a copy of an interception warrant or the relevant parts of the warrant, or evidence of any other lawful interception authority, to assist the surveillance agency to whom the warrant is issued or the authority is granted.

Clause 14 provides that 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.

Part 3

Miscellaneous provisions

Transitional provision

Clause 15 is a transitional provision. It provides that, except for any interception capability on a public telecommunications network or a telecommunications service that was already in place or that was the subject of an agreement between the Crown and a network operator before the commencement of the Bill, the requirement to have an interception capability applies only,--

- in the case of a public switched telephone network or a telecommunication service, on or after 1 October 2004; and
- in the case of a public data network, on or after 1 April 2008.

Allocation of costs relating to interception capability

Clause 16 provides for the allocation of costs relating to interception capability on a public switched telephone network or a telecommunications service. These costs are to be allocated between the Crown and network operators.

Clause 17 relates to the costs of interception capability on a public data network.

Costs relating to interceptions

Clause 18 requires a surveillance agency to pay for the actual and reasonable costs incurred by a network operator or a service provider in providing assistance to the agency under *clause 13*.

Resolution of disputes about costs

Clause 19 sets out a process for resolving disputes about costs.

Protection from liability

Clause 20 excludes certain persons from liability 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 the Bill.

Compliance orders

Clause 21 enables the High Court to make a compliance order requiring any person who has not complied with any of the duties imposed by *Part 2* to do any specified thing or to cease any specified activity.

Clause 22 relates to applications for a compliance order.

Clause 23 gives an applicant for a compliance order and the person against whom the order is sought the right to be heard.

Clause 24 relates to the decision on an application for a compliance order.

Appeals against making of compliance order

Clause 25 provides that a party to proceedings relating to an application for a compliance order or any person prejudicially affected may, with the leave of the Court of Appeal, appeal to that court.

Clause 26 provides that, unless the Court of Appeal otherwise directs, the operation of a compliance order is not suspended by an appeal, and the order may be enforced as if the appeal were not pending.

Enforcement

Clause 27 allows the High Court, on the application of a surveillance agency, to impose a pecuniary penalty payable to the Crown if that court is satisfied that a person has acted in contravention of a compliance order.

Regulations

Clause 28 authorises the making of regulations.

Regulatory impact and compliance cost statement

Statement of the public policy objective

The primary objective of this Bill is to ensure that surveillance agencies are able, if required under an interception warrant or any other lawful interception authority, to--

- intercept telecommunications; and

- investigate serious offences; and
- help protect national security.

Statement of problem and need for action

Changes in telecommunications technology have meant that surveillance agencies are now unable to intercept some telecommunications, despite having the legal authority to do so. Organised criminals are aware of this and these proposals are necessary to prevent law enforcement and national security capability being seriously eroded.

Statement of options for achieving the desired objective

The alternative to the proposed legislative amendments is for the surveillance agencies to seek the agreement of telecommunications network operators to change their systems. As technology is regularly upgraded, and as more companies enter the market, this is not considered a robust or cost-effective approach.

Statement of the net benefit of this proposal

Benefits

The benefits of legislating are unquantifiable, but include--

- sustaining the ability of surveillance agencies to investigate serious crime and threats to national security; and
- the likelihood of being the least costly approach to maintaining interception capability because companies will have advance notice of these requirements and can build them into new services or systems from the outset. It will be in the companies' interests to keep the costs to a minimum to the extent they are able to do this; and
- all the relevant companies are treated on a similar basis.

Costs

Compliance costs

The Bill--

- imposes greater compliance costs on telecommunications network operators (which are all privately owned companies), unless the Government is required to meet all the costs; and
- could provide a barrier to entry, thereby limiting competition, if the compliance costs for new entrants were too high; and
- could impede or delay the introduction of new telecommunications technologies if the interception capability requirements were difficult to achieve.

Financial costs

The costs to the Government are estimated to be up to $3 million. The Government will meet the costs of modifying existing fixed and mobile voice networks only, and telecommunications companies will meet the costs of installing and maintaining the capability for other services and for any new services within the timeframe specified in the legislation. (Essentially this option means the Government covers costs of upgrading existing telephone services but not the costs for upgrading networks to provide for the

interception of Internet and email services.)

Compliance costs

The compliance costs are estimated at about $12 million over 5 years, plus costs for future services. Compliance costs for new services should be less than the costs of modifications to an existing network and in some cases may be difficult to isolate from the general cost of developing the service. The phased implementation for existing services should help manage and reduce costs. In addition, compliance costs are likely to fall over time as more countries require interception capability and equipment manufacturers incorporate interception options to meet international requirements for such capabilities. The United States, European countries, and Australia are pursuing "international user requirements", which would require interception capability to be a standard design feature of new technology.

Consultation

The following agencies have been consulted:

Department of Prime Minister and Cabinet

Government Communications Security Bureau

Ministry of Economic Development

New Zealand Police

New Zealand Security Intelligence Service

Office of the Privacy Commissioner

State Services Commission

Treasury.

The proposals have been discussed with the following telecommunications companies:

City Link

Clear

Tangent

Team Talk

Telecom

Vodafone.

Hon Lianne Dalziel

Telecommunications (Interception Capability) Bill

Government Bill

Contents

The Parliament of New Zealand enacts as follows:

1 Title

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

Part 1--Preliminary provisions

General

2 Commencement

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

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

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

(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

(c) does not include the content of the telecommunication

"compliance order" means an order made by the High Court under section 21

"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 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 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 of the Misuse of Drugs Amendment Act 1978:

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

"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

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

"number"--

(a) means the address used for the purposes of a telecommunication; and

(b) includes any of the following:

(i) a telephone number:

(ii) a mobile telephone number:

(iii) an Internet address:

(iv) 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

(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

"public data network"–

(a) means a data network used, or intended for use, in whole or in part, by the public; and

(b) includes, without limitation, the following facilities:

(i) the Internet:

(ii) email

"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

"public telecommunications network" means--

(a) a public switched telephone network; and

(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

(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

(b) does not include a network operator

"surveillance agency" means--

(a) a law enforcement agency; or

(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

(b) includes a telephone device.

(2) In this Act, unless the context otherwise requires, **"network"**, **"telecommunication"**, **"telecommunications service"**, and **"telephone device"** have the meanings given to them by section 5 of the Telecommunications Act 2001.

4 Act binds the Crown

This Act binds the Crown.

Purpose and principles

5 Purpose

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

(c) that network operators and service providers have the freedom to choose system design features and specifications that are appropriate for their own purposes.

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:

(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.

Part 2--Interception duties

Duty to have interception capability

7 Network operators must ensure public telecommunications networks and telecommunications services have interception capability

(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.

(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.

8 When duty to have interception capability is complied with

(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 on that network or service is able to--

(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 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

(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

(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.

(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--

(a) the content of that telecommunication has been encrypted; and

(b) the network operator intercepting the telecommunication has provided that encryption.

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

Limits on duty to have interception capability

9 Certain facilities excluded from scope of duty under section 7

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

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.

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.

(2) The Minister may grant the exemption--

(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

(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.

(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

(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),--

(a) in the case of an interception warrant issued to an intelligence and security agency, a copy of the relevant parts of the warrant:

(b) in any other case, a copy of the warrant or evidence of the authority.

(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--

(a) making available any of the person's officers, employees, or agents who are able to provide any technical assistance that may be reasonably necessary for the agency to intercept a telecommunication that is subject to the warrant or authority; and

(b) taking all other steps that are reasonably necessary for the purpose of giving effect to the warrant or authority.

14 Duty to minimise impact of interception on third parties

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.

Part 3--Miscellaneous provisions

Transitional provision

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

(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,--

(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.

(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.

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:

(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

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 after the date of the invoice or other appropriate document.

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,--

(a) in the case of costs under sections 16 and 17, the Crown and a network operator; and

(b) in the case of costs under section 13, a surveillance agency and a network operator or a service provider.

(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--

(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

(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.

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--

(a) to do any specified thing; or

(b) to cease any specified activity.

(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.

23 Right to be heard

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

(a) hear the applicant; and

(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--

(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.

(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.

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

(b) every compliance order may be enforced in the same manner and in all respects as if that appeal were not pending.

Enforcement

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.

(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 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.

Regulations

28 Regulations

(1) The Governor-General may, by Order in Council, make regulations for all or any of the following purposes:

(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) {sic ? 8(1)(a) } or (b):

(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).

(2) Before recommending the making of an Order in Council under subsection (1), the Minister must--

(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

(b) in relation to regulations made under subsection (1)(c), consult with the Privacy Commissioner appointed under the Privacy Act 1993.

(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.