Reprint
as at 6 April 2004

Telecommunications (Interception Capability) Act 2004

Public Act	2004 No 19
Date of assent	5 April 2004
Commencement	see section 2

Contents

Note
Changes authorised by section 17C of the Acts and Regulations Publication Act 1989 have been made in this reprint.

A general outline of these changes is set out in the notes at the end of this reprint, together with other explanatory material about this reprint.

This Act is administered by the Ministry of Justice.

---

1 Title

This Act is the Telecommunications (Interception Capability) Act 2004.

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, 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 312CD 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:
(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

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

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
  (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:
  (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:
  (vi) an email address

other lawful interception authority—
(a) means an authority—

(i) 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

(ii) 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; and

(b) includes an authority to intercept a private communication (whether in an emergency situation or otherwise) that is granted to any member of a surveillance agency under any other enactment

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) 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

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**, **telecommunication link**, **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) 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

(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.

(3) 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 telecom-

munications 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 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) 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.

(3) A network operator must, in order to comply with subsection (l)(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.

(4) However, subsection (3) does not require a network operator to—

(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—

(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.

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 on a telecommunication link that is used to interconnect 2 or more 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; or

(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 reasonable technical assistance that may be necessary for the agency to intercept a telecommunication that is subject to the warrant or authority; and

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

(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

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) 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,—

(a) in the case of a public switched telephone network or a telecommunications service, 18 months after that commencement; and

(b) in the case of a public data network, 5 years after that commencement.

(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; 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

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 1 month 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; or

(b) in the case of costs under section 18, 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 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):

(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:

(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.

(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.

Contents

Notes

1 General

This is a reprint of the Telecommunications (Interception Capability) Act 2004. The reprint incorporates all the amendments to the Act as at 6 April 2004, as specified in the list of amendments at the end of these notes.

Relevant provisions of any amending enactments that have yet to come into force or that contain relevant transitional or savings provisions are also included, after the principal enactment, in chronological order.

2 Status of reprints

Under section 16D of the Acts and Regulations Publication Act 1989, reprints are presumed to correctly state, as at the date of the reprint, the law enacted by the principal enactment and by the amendments to that enactment. This presumption applies even though editorial changes authorised by section 17C of the Acts and Regulations Publication Act 1989 have been made in the reprint.

This presumption may be rebutted by producing the official volumes of statutes or statutory regulations in which the principal enactment and its amendments are contained.

3 How reprints are prepared

A number of editorial conventions are followed in the preparation of reprints. For example, the enacting words are not included in Acts, and provisions that are repealed or revoked are omitted.

For a detailed list of the editorial conventions, *see* http://www.pco.parliament.govt.nz/legislation/reprints.shtml or Part 8 of the *Tables of Acts and Ordinances and Statutory Regulations, and Deemed Regulations in Force*.

4 Changes made under section 17C of the Acts and Regulations Publication Act 1989

Section 17C of the Acts and Regulations Publication Act 1989 authorises the making of editorial changes in a reprint as set out in sections 17D and 17E of that Act so that, to the extent permitted, the format and style of the reprinted enactment is consistent with current legislative drafting practice. Changes that would alter the effect of the legislation are not permitted.

A new format of legislation was introduced on 1 January 2000. Changes to legislative drafting style have also been made since 1997, and are ongoing. To the extent permitted by section 17C of the Acts and Regulations Publication Act 1989, all legislation reprinted after 1 January 2000 is in the new format for legislation and reflects current drafting practice at the time of the reprint.

In outline, the editorial changes made in reprints under the authority of section 17C of the Acts and Regulations Publication Act 1989 are set out below, and they have been applied, where relevant, in the preparation of this reprint:

- omission of unnecessary referential words (such as "of this section" and "of this Act")
- typeface and type size (Times Roman, generally in 11.5 point)
- layout of provisions, including:
  - indentation
  - position of section headings (eg, the number and heading now appear above the section)
- format of definitions (eg, the defined term now appears in bold type, without quotation marks)
- format of dates (eg, a date formerly expressed as "the 1st day of January 1999" is now expressed as "1 January 1999")

- position of the date of assent (it now appears on the front page of each Act)
- punctuation (eg, colons are not used after definitions)
- Parts numbered with roman numerals are replaced with arabic numerals, and all cross-references are changed accordingly
- case and appearance of letters and words, including:
  - format of headings (eg, headings where each word formerly appeared with an initial capital letter followed by small capital letters are amended so that the heading appears in bold, with only the first word (and any proper nouns) appearing with an initial capital letter)
  - small capital letters in section and subsection references are now capital letters
- schedules are renumbered (eg, Schedule 1 replaces First Schedule), and all cross-references are changed accordingly
- running heads (the information that appears at the top of each page)
- format of two-column schedules of consequential amendments, and schedules of repeals (eg, they are rearranged into alphabetical order, rather than chronological).

5 List of amendments incorporated in this reprint (most recent first)

Wellington, New Zealand:
Published under the authority of the New Zealand Government—2009