Government Communications Security Bureau Bill

Government Bill

As reported from the Intelligence and Security Committee

Commentary

Recommendation

The Intelligence and Security Committee has examined the Government Communications Security Bureau Bill and recommends that it be passed with the amendments shown in the Bill.

Conduct of the examination

The Government Communications Security Bureau Bill was referred to the Intelligence and Security Committee on 8 May 2001. The closing date for submissions was 30 June 2001. The Committee received and considered 16 submissions from a range of interested groups and individuals. Four submissions were heard orally. One and a half hours were spent on the hearing of evidence and consideration took a further 1 hour.

We were required to report back by 7 November 2001.

Advice was received from the Department of the Prime Minister and Cabinet and the Government Communications Security Bureau.

This commentary sets out the details of the Committee's consideration of the Bill and the major issues addressed by the committee.

Background to the Bill

The key features of the Government Communications Security Bureau Bill are:

- The establishment of the Government Communications Security Bureau (GCSB) as a department of State;
- The definition of the objective and functions of the GCSB;
- The regulation of the GCSB's functions with respect to the interception of communications; and
- The creation of a regime of interception warrants and computer access authorisations in relation to the activities of the GCSB.

Definitions

Several submissions raised concerns about definitions contained in the Bill, in particular, the terms "foreign communications" and "foreign organisation". Some submissions considered that the term "foreign organisation" was too widely drafted and should be re-defined in such a way as to limit the GCSB's ability to intercept the communications of international organisations in which New Zealand persons may be involved. The Committee carefully considered these arguments, and concluded that sufficient safeguards exist to ensure the privacy of New Zealand persons, making further amendment unnecessary.

The Committee does, however, consider that an amendment to the definition of "foreign person" in clause 4 is required to make it clear that a person acting in his or her capacity as an agent or a representative of an individual who is neither a New Zealand citizen nor a permanent resident is considered to be a foreign person.

Objective of the GCSB

Some submitters were concerned that the objectives stated in clause 7 of the Bill were too vague. One submission argued that a "strict necessity" test should be adopted to constrain the Bureau's intelligence collection operations to those activities necessary for the protection of New Zealand interests, as distinct from advancing those interests. The Committee does not agree with this proposition.

As a separate matter, the Inspector-General of Intelligence and Security who wrote to the Director GCSB directly to provide his

comments on the Bill, noted that there was no explicit authorisation for co-operation with overseas partner agencies regarding dissemination of legitimately collected intelligence. We have agreed that this concern should be met by inserting a new objective into clause 7(1) and by a subsequent amendment to clause 8(1)(d). The new objective is to read: "The objective of the Bureau is to contribute to the national security of New Zealand by providing . . . (ab) foreign intelligence to meet international obligations and commitments of the Government of New Zealand". The consequential need to amend the functions of the GCSB is met by inserting in clause 8(1)(d) the words "whether in New Zealand or abroad" after "office holder".

Functions of the GCSB

One submission raised the possibility of an enhanced role for the Inspector-General of Intelligence and Security in relation to the foreign intelligence requirements. Another raised concerns about the balance between the GCSB's functions and the protection of those rights and freedoms affirmed in the New Zealand Bill of Rights Act 1990. The Committee carefully considered these concerns, but decided that the former was not and should not be part of the Inspector-General's role, and that the latter had already been sufficiently considered by the Ministry of Justice prior to the Bill's introduction.

Annual report

A number of submissions sought the inclusion in the GCSB's published annual report of additional information concerning the Bureau's operational activities. While the committee considers that the inclusion of such information would be prejudicial to security, we did, however, agree with the Privacy Commissioner that a minor amendment might usefully be made to clause 12(4)(e), by inserting the word "unreasonably" after the word "prejudice".

Interceptions not to target domestic communications

One submission argued that, in light of the New Zealand Bill of Rights Act 1990, all people in New Zealand should be given protection from having their communications intercepted, regardless of nationality. The committee does not agree with this concept.

Interceptions for which warrant or authorisation required

The committee agreed with the Privacy Commissioner that clause 15(1)(b) requires minor amendment in order to make it clear that in certain cases occupier consent is not a substitute for obtaining an interception warrant.

Certain interceptions permitted without interception warrant

One submission sought the explicit naming in clause 16(1) of enactments that authorise the GCSB to intercept foreign communications without a warrant. While the committee does not agree, we note in this report for the record that the words "by another enactment" currently refer to the Crimes Act 1961 and the Radiocommunications Act 1989.

Duty to minimise impact of interception on third parties

One submitter sought extension of the duty to minimise the impact of interception on third parties to persons making interceptions under computer access authorisations, and to interceptions undertaken without the authority of a warrant. The committee agreed that the extension was a necessary safeguard, and concluded that clause 19 should be deleted and a new clause 24A inserted accordingly.

Term of warrant or authorisation

Some submissions considered that the warrant or authorisation period should be limited to six months or less. After careful consideration, the committee concluded that the twelve-month period, which is consistent with corresponding provisions in the New Zealand Security Intelligence Service Act 1969, should stand.

Destruction of irrelevant records obtained by interception

One submitter considered that the GCSB should also be required to destroy *relevant* records obtained by interception when there is no longer any lawful reason to retain them. In order to achieve this, he sought either an explicit provision in the Bill or the revocation of the GCSB's exemption from Information Privacy Principle 9 of the

Privacy Act 1993. The Committee considered the latter approach to be the best way to achieve the desired result. Another submitter raised a concern that the words "is relevant to" in the phrase ". . . except to the extent that the information recorded in the copy or record is relevant to . . ." in clause 24(1) are too broad. The Committee agreed to replace the words "is relevant to" with the expression "relates directly or indirectly to", following the wording in section 4G of the New Zealand Security Intelligence Service Act 1969.

Revocation

One submitter noted that it may not be necessary to include clause 35 in the Bill, given that clause 27 of Supplementary Order Paper No 85, containing the proposed amendments to the Crimes Amendment Bill (No 6), has already been introduced into Parliament to revoke the Crimes (Exemption of Listening Device) Order 1997. This is a question of timing which will be addressed at the appropriate point in the parliamentary process.

Other issues

Clause 2 of the Bill requires amendment, as section 133A of the Radiocommunications Act 1989 is now in force. The Committee agreed that a further amendment to that section should be made, in order to address a drafting issue; this is achieved by clause 32(3) of the Bill.

We have concluded that clause 4 of the Bill requires amendment so that the definition of "computer system" is consistent with a change made to the Crimes Amendment Bill (No 6) by Supplementary Order Paper No 85. This results in a minor consequential amendment to clauses 15(2) and 20(1).

We also note that the Crimes Amendment Bill (No 6) includes a qualified exemption for the GCSB to the new offence of unauthorised access to a computer or computer system. This exemption preserves the GCSB's existing foreign intelligence collection capabilities, for which no warrant is required. We have concluded that the Bill requires amendment to ensure consistency with the Crimes Amendment Bill (No 6) in this respect; this is achieved by an amendment to clause 16(2), with a consequential amendment to clause 16(1). The effect of these provisions is that the GCSB will

retain its existing legal authority to intercept *foreign* private communications, which are transmitted through or between computers or computer systems.

Key to symbols used in reprinted bill

As reported from Intelligence and Security Committee

Struck out (unanimous) Subject to this Act,	Text struck out unanimously
New (unanimous) Subject to this Act,	Text inserted unanimously
(Subject to this Act,)	Words struck out unanimously
Subject to this Act,	Words inserted unanimously

Rt Hon Helen Clark

Government Communications Security Bureau Bill

Government Bill

Contents

The Parliament of New Zealand enacts as follows:

1 Title

This Act is the Government Communications Security Bureau Act **2001**.

Part 1
Preliminary provisions

2 Commencement

This Act ((*other than* ***section 32***)) comes into force on the day after the date on which it receives the Royal assent.

Struck out (unanimous)

(2) **Section 32** comes into force on the day on which section 133A of the Radiocommunications Act 1989 comes into force.

3 Purpose

The purpose of this Act is to—

(a) continue the Government Communications Security Bureau and establish it as a department of State:

(b) specify the objective and functions of the Bureau:

(c) specify the circumstances in which the Bureau requires an interception warrant or a computer access authorisation to intercept foreign communications:

(d) specify the conditions that are necessary for the issue of an interception warrant or a computer access authorisation and the matters that may be authorised by a warrant or an authorisation:

(e) specify the circumstances in which the Bureau may use interception devices to intercept foreign communications without a warrant or an authorisation.

4 Interpretation

In this Act, unless the context otherwise requires,—

access, in relation to any computer system, means instruct, communicate with, store data in, retrieve data from, or otherwise make use of any of the resources of the computer system

Bureau means the Government Communications Security Bureau continued by **section 6**

communication includes signs, signals, impulses, writing, images, sounds, or data that a person or machine produces, sends, receives, processes, or holds in any medium

computer access authorisation or **authorisation** means an authorisation issued under **section 20**

computer system—

(a) means—

(i) a computer; or

(ii) 2 or more interconnected computers; or

(iii) any communication links between computers or to remote terminals or any other device; or

(iv) 2 or more interconnected computers combined with any communication links between computers or to remote terminals or any other device; and

(b) includes any part of the items described in **paragraph (a)** and all related input, output, processing, storage, software, or communication facilities, and stored data

Director means the chief executive of the Bureau; and includes a person who, under **section 10**, exercises or performs the functions, duties, or powers of the Director

foreign communications means communications that contain, or may reasonably be expected to contain, foreign intelligence

foreign intelligence means information about the capabilities, intentions, or activities of a foreign organisation or a foreign person

foreign organisation means—

(a) a Government of any country other than New Zealand:

(b) an entity controlled by the Government of any country other than New Zealand:

(c) a company or body corporate that is incorporated outside New Zealand, or any company within the meaning of the Companies Act 1993 that is, for the purposes of the Companies Act 1993, a subsidiary of any company or body corporate incorporated outside New Zealand:

(d) an unincorporated body of persons consisting exclusively of foreign organisations or foreign persons that carry on activities wholly outside New Zealand:

(e) an international organisation:

(f) a person acting in his or her capacity as an agent or a representative of any Government, body, or organisation referred to in any of **paragraphs (a) to (e)**

foreign person means an individual who is neither a New Zealand citizen nor a permanent resident; and includes a person acting in his or her capacity as an agent or a representative of such an individual

intercept includes hear, listen to, record, monitor, acquire, or receive a communication, or acquire its substance, meaning, or sense

interception device means any electronic, mechanical, electromagnetic, optical, or electro-optical instrument, apparatus, equipment, or other device that is used or is capable of being used to intercept communications

interception warrant means a warrant issued under **section 17**

medium means any form in which communications may be produced, sent, received, processed, or held; and includes electromagnetic, acoustic, or other energy

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

network has the same meaning as in section 2(1) of the Telecommunications Act 1987; but does not include a line (within the meaning of that Act) that is used exclusively by the Bureau

permanent resident means a person who is, or who is deemed to be, the holder of a residence permit under the Immigration Act 1987

private communication—

(a) means a communication between 2 or more parties made under circumstances that may reasonably be taken to indicate that any party to the communication desires it to be confined to the parties to the communication; but

(b) does not include a communication occurring in circumstances in which any party ought reasonably to expect that the communication may be intercepted by some

other person not having the express or implied consent of any party to do so

serious crime means,—

(a) in relation to New Zealand, any indictable offence; and

(b) in relation to an overseas country, any offence that, if it occurred in New Zealand, would be an indictable offence.

5 Act binds the Crown

This Act binds the Crown.

Part 2
Organisation, objectives, and functions of Bureau

6 Bureau continued and established as department

(1) There continues to be an instrument of the Executive Government of New Zealand known as the Government Communications Security Bureau.

(2) On and from the commencement of this Act, the Bureau is a department of State.

7 Objective of Bureau

(1) The objective of the Bureau is to contribute to the national security of New Zealand by providing—

(a) foreign intelligence that the Government of New Zealand requires to protect and advance—

(i) the security or defence of New Zealand; or

(ii) the international relations of the Government of New Zealand; or

(iii) New Zealand's international well-being or economic well-being; and

New (unanimous)

(ab) foreign intelligence to meet international obligations and commitments of the Government of New Zealand; and

(b) advice, assistance, and protection to departments of State and other instruments of the Executive Government of New Zealand in order to—

(i) protect and enhance the security of their communications, information systems, and computer systems; or

(ii) protect their environments from electronic or other forms of technical surveillance by foreign organisations or foreign persons.

(2) For the purposes of **subsection (1)(a)(iii)**, the interests of New Zealand's international well-being or economic well-being are relevant only to the extent that they are affected by the actions or intentions of foreign organisations or foreign persons.

8 Functions of Bureau

(1) The Bureau has the following functions:

(a) to gather foreign intelligence, in accordance with the foreign intelligence requirements of the Government of New Zealand,—

(i) by intercepting communications under the authority of this Act; or

(ii) by co-operating with public authorities or other entities in New Zealand and abroad; or

(iii) by collecting information in any other lawful manner:

(b) to decipher, decode, and translate foreign communications:

(c) to examine and analyse foreign communications and foreign intelligence:

(d) to provide reports on foreign intelligence to the Minister and any person or office holder, whether in New Zealand or abroad, authorised by the Minister:

(e) to co-operate with, or to provide advice and assistance to, any public authority or other entity, in New Zealand or abroad,—

(i) on the protection of information that the public authority or other entity produces, sends, receives, or holds in any medium; or

(ii) on any matter that is relevant—

(A) to the functions of the public authority or other entity; and

(B) to any purpose specified in **subsection (2)**.

(2) The Bureau may perform its functions only for the following purposes:

(a) to pursue its objective:

(b) to protect the safety of any person:

(c) in support of the prevention or detection of serious crime.

(3) The performance of the Bureau's functions is subject to the control of the Minister.

9 Director of Bureau

(1) The Director of the Bureau is appointed by the Governor-General.

(2) The remuneration of the Director is determined by the Higher Salaries Commission under the Higher Salaries Commission Act 1977.

(3) The Director holds office during the pleasure of the Governor-General and is subject to any conditions (other than remuneration) determined by the Minister.

(4) Despite **subsection (3)**, the person who, at the commencement of this Act, holds office as Director—

(a) continues to hold that office in accordance with the person's contract of employment; and

(b) until a determination of the kind referred to in **subsection (2)** is made in respect of the person, continues to be remunerated in accordance with that contract; and

(c) is eligible to be reappointed as Director.

10 Acting Director

(1) When there is a vacancy in the position of Director or when the Director is (for whatever reason) absent from duty, the functions, duties, and powers of the Director must be exercised or performed by a person whom the Minister directs to exercise or perform those functions, duties, and powers.

(2) The Minister may give a direction before the occurrence of any vacancy or absence referred to in **subsection (1)** or while the vacancy or absence continues.

(3) No direction and no act done by a person acting under a direction given under this section may, in a proceeding, be

questioned on the ground that the occasion for the direction had not arisen or had ceased, or on the ground that the person had not been appointed to a position to which the direction relates.

11 Prohibition on unauthorised disclosure of information

(1) A person who is or was an employee of the Bureau may not disclose or use any information gained by or conveyed to the person through the person's connection with the Bureau except in the strict course of the person's official duties or as authorised by the Minister.

(2) Every person commits an offence and is liable on summary conviction to imprisonment for a term not exceeding 2 years or to a fine not exceeding $2,000 who contravenes **subsection (1)**.

Compare: 1969 No 24 s 12A(1), (4)

12 Annual report

(1) As soon as practicable after each year ending on 30 June, the Director must deliver to the Minister a report on the activities of the Bureau during that year.

(2) When the Minister receives a copy of a report under **subsection (1)**, the Minister must, without delay, submit a copy of the report to the members of the Intelligence and Security Committee established under the Intelligence and Security Committee Act 1996.

(3) Within 30 sitting days after receiving the report under **subsection (1)**, the Minister must present to the House of Representatives a copy of the report that accords with any directions given under **subsection (4)**, and includes—

(a) the statement specified in section 39(3) of the Public Finance Act 1989 as set out in section 70I of that Act; and

(b) a statement as to whether or not any interception warrants were in force during the year to which the report relates; and

(c) a statement as to whether or not any computer access authorisations were in force during the year to which the report relates; and

(d) a statement setting out—

(i) a summary of the Bureau's equal employment opportunities programme for the year to which the report relates; and

(ii) an account of the extent to which the Bureau was able to meet, during the year to which the report relates, the equal employment opportunities programme for that year.

(4) Before presenting a copy of the report to the House of Representatives under **subsection (3)**, the Minister may direct that any material (other than the material referred to in **subsection (3)(a) to (d)**) be deleted from the report if the Minister considers that the material is likely—

(a) to prejudice the security or defence of New Zealand or the international relations of the Government of New Zealand; or

(b) to prejudice the entrusting of information to the Government of New Zealand on a basis of confidence by the Government of any other country or any agency of such a Government; or

(c) to prejudice the entrusting of information to the Government of New Zealand on a basis of confidence by any international organisation; or

(d) to endanger the safety of any person; or

(e) to prejudice unreasonably the privacy of an individual.

Compare: 1969 No 24 s 4J

Part 3
Interception of communications

Purpose of Part

13 Purpose of Part

The purpose of this Part is,—

(a) subject to the restrictions imposed by this Part, to enable the Bureau to obtain foreign intelligence; and

(b) to authorise the interception of communications (whether under **section 16** or under an interception warrant or a computer access authorisation) only if the purpose of the interception is to obtain foreign intelligence.

Restrictions imposed on interceptions

14 Interceptions not to target domestic communications

Neither the Director, nor an employee of the Bureau, nor a person acting on behalf of the Bureau may authorise or take any action for the purpose of intercepting the communications of a person (not being a foreign organisation) who is a New Zealand citizen or a permanent resident.

15 Interceptions for which warrant or authorisation required

(1) Unless authorised by an interception warrant to do so, neither the Director, nor an employee of the Bureau, nor a person acting on behalf of the Bureau may—

(a) physically connect an interception device to any part of a network; or

Struck out (unanimous)

(b) install an interception device in a place—

(i) without the permission of the occupier of the place; or

(ii) for the purpose of intercepting communications made or received in the place.

New (unanimous)

(b) install an interception device in a place for the purpose of intercepting communications that occur in the place.

(2) Unless authorised by **section 16** or by a computer access authorisation to do so, neither the Director, nor an employee of the Bureau, nor a person acting on behalf of the Bureau may access a computer system (*or part of a computer system*) that the person concerned is not otherwise authorised to access.

16 Certain interceptions permitted without interception warrant or computer access authorisation

(1) The Director, or an employee of the Bureau, or a person acting on behalf of the Bureau may, without an interception warrant,

or, as the case requires, without a computer access authorisation, intercept foreign communications only if the interception is authorised by this Act or by another enactment.

(2) The Director, or an employee of the Bureau, or a person acting on behalf of the Bureau may, without an interception warrant, or, as the case requires, without a computer access authorisation, intercept foreign communications by using an interception device, but only if—

(a) the interception does not involve any activity specified in **section 15(1)**; and

New (unanimous)

(ab) any access to a computer system is limited to access to 1 or more communication links between computers or to remote terminals; and

(b) the interception is carried out by the Director or with the authority of the Director for the purpose of obtaining foreign intelligence; and

(c) the foreign communications do not contain private communications other than private communications that—

(i) are produced, sent, or received by, or sent to, a foreign organisation or a foreign person; and

(ii) contain, or may reasonably be expected to contain, foreign intelligence.

(3) This section is subject to **section 14**.

Interception warrants

17 Issue of interception warrant

(1) The Director may apply in writing to the Minister for the issue of an interception warrant authorising the use of interception devices to intercept communications not otherwise lawfully obtainable by the Bureau.

(2) If satisfied on evidence given on oath by the Director that the conditions specified in **subsection (3)** apply to the proposed warrant, the Minister may issue the warrant to authorise the interception of either or both of the following kinds of communication:

(a) foreign communications made or received by 1 or more persons specified in the warrant or made or received in 1 or more places specified in the warrant:

(b) foreign communications that are sent from, or are being sent to, an overseas country.

(3) The conditions referred to in **subsection (2)** are that—

(a) the interception to be authorised by the proposed warrant is essential for the protection or advancement of 1 or more of the interests specified in **section 7(1)(a)**; and

(b) the value of the information sought to be obtained under the proposed warrant justifies the particular interception; and

(c) the information is not likely to be obtained by other means; and

(d) if the communications to be intercepted are of the kind specified in **subsection (2)(a)**, that there are reasonable grounds for believing—

(i) that any person specified in the proposed warrant as a person whose communications may be intercepted is a foreign person or a foreign organisation; and

(ii) that any place to be specified in the proposed warrant is occupied by a foreign organisation or a foreign person.

(4) Before issuing a warrant, the Minister must consult the Minister of Foreign Affairs and Trade about the proposed warrant.

(5) The Minister may issue a warrant subject to any conditions that the Minister considers advisable in the public interest.

(6) This section is subject to **section 14**.

Compare: 1969 No 24 ss 4A(2)–(5), 4B(3)

18 Persons acting under warrant

(1) Every interception warrant must specify the person or class of person who may make the interception authorised by the warrant.

(2) A warrant may also request 1 or more persons or class of persons to give any assistance that is reasonably necessary to give effect to the warrant.

(3) If a request is made, under **subsection (2)**, to 1 or more persons or class of persons who are employees (the **employees**), the

warrant must also request the persons who are the employers of the employees, or any other persons in any way in control of the employees, to make the services of the employees available to the Bureau.

(4) On an application made in writing by the Director, the Minister may amend a warrant—

(a) by substituting another person for the person specified in the warrant under **subsection (1)**:

(b) by substituting another person or another class of persons for a person or class of persons requested under **subsection (2)**:

(c) by adding any person or class of persons to the persons requested under **subsection (2)**.

Compare: 1969 No 24 s 4D

Struck out (unanimous)

19 Duty to minimise impact of interception on third parties

Every person who, under an interception warrant, intercepts or assists in intercepting the communications of 1 or more persons specified in the warrant must take all practicable steps that are reasonable in the circumstances to minimise the likelihood of intercepting communications that are not relevant to the persons whose communications are to be intercepted.

Compare: 1969 No 24 s 4F(1)

Computer access authorisation

20 Authorisation to access computer system

(1) The Minister may, on the written application of the Director, authorise the Director or a specified employee, or a specified class of employees, of the Bureau to access a computer system (*or part of computer system*) of a specified foreign organisation or foreign person.

(2) Before the Minister grants an authorisation, he or she must be satisfied on evidence given on oath by the Director that—

(a) the access to be authorised is essential for the protection or advancement of 1 or more of the interests specified in **section 7(1)(a)**; and

(b) that the persons whose computer system is to be accessed are foreign persons or foreign organisations; and

(c) the value of the information sought to be obtained under the authorisation justifies the access; and

(d) the information is not likely to be obtained by other means.

(3) Every authorisation must be in writing.

(4) Before issuing an authorisation, the Minister must consult the Minister of Foreign Affairs and Trade about the proposed authorisation.

(5) The Minister may issue an authorisation subject to any conditions that the Minister considers advisable in the public interest.

Provisions applicable to (warrants and authorisations) warrants, authorisations, and powers under section 16

21 Director's functions in relation to warrants and authorisations not to be delegated

Despite section 41 of the State Sector Act 1988, the Director may not delegate to any person the Director's functions under **section 17 or section 20**.

22 Action taken in accordance with warrant or authorisation justified

(1) Every person who is authorised to give effect, or to assist in giving effect, to an interception warrant or to a computer access authorisation is justified in taking, in accordance with the terms and conditions of the warrant or authorisation, any reasonable action necessarily involved in giving, or assisting to give, effect to the warrant or authorisation.

(2) In any proceedings, a certificate by the Attorney-General as to any matters specified in a warrant or authorisation is sufficient evidence of those matters and, if such a certificate is produced, it is not necessary to produce the warrant or authorisation to which the certificate relates.

Compare: 1969 No 24 s 4A(6), (7)

23 Term of warrant or authorisation

(1) Every interception warrant and every computer access authorisation must specify a period not exceeding 12 months for which the warrant or authorisation is valid.

(2) The expiry of an interception warrant or of an authorisation does not prevent a further application for an interception warrant or an authorisation in respect of the same subject matter.

Compare: 1969 No 24 s 4(A)C

24 Destruction of irrelevant records obtained by interception

(1) Every person who intercepts any communication under **section 16** or under an interception warrant or a computer access authorisation must, as soon as practicable after the interception, destroy any copy that he or she may make of the communication, or any part of the communication, and any record, whether in writing or otherwise, of the information obtained by that interception, except to the extent that the information recorded in the copy or record (*is relevant*) relates directly or indirectly to—

(a) the protection or advancement of 1 or more of the interests specified in **section 7(1)(a)**; or

(b) any of the Bureau's functions under **section 8**.

(2) Every person commits an offence and is liable on summary conviction to a fine not exceeding $1,000 who knowingly fails to comply with **subsection (1)**.

Compare: 1969 No 24 s 4G

New (unanimous)

24A Duty to minimise impact of interception on third parties

Every person who, in accordance with **section 16** or with an interception warrant or with a computer access authorisation, intercepts or assists in intercepting the communications of 1 or more persons must take all practicable steps that are reasonable in the circumstances to minimise the likelihood of intercepting communications that are not relevant to the persons whose communications are to be intercepted.

Compare: 1969 No 24 s 4F(1)

25 Prevention or detection of serious crime

Despite **section 24**, the Director, for the purpose of preventing or detecting serious crime in New Zealand or in any other country, may retain any information that comes into the possession of the Bureau and may communicate that information to members of the New Zealand Police or to any other persons, and in any manner, that the Director thinks fit.

Compare: 1969 No 24 s 4H

Part 4
Provisions relating to other enactments

26 Amendment to Crimes Act 1961

(1) Section 216B(2)(b) of the Crimes Act 1961 is amended by inserting, after subparagraph (iii), the following subparagraph:

"(iiia) the Government Communications Security Bureau Act **2001**; or".

(2) Section 216D(2) of the Crimes Act 1961 is amended by inserting, after the words "New Zealand Security Intelligence Service" in both places where they appear, the words "or the Government Communications Security Bureau".

27 Amendment to Higher Salaries Commission Act 1977

The Fourth Schedule of the Higher Salaries Commission Act 1977 is amended by inserting, after the item relating to the Chief of the Employment Relations Authority and other members of the Employment Relations Authority, the item "Director of the Government Communications Security Bureau."

28 Amendment to Inspector-General of Intelligence and Security Act 1996

Section 11(1) of the Inspector-General of Intelligence and Security Act 1996 is amended by inserting, after paragraph (d), the following paragraph:

"(da) without limiting the generality of paragraph (a), to review the effectiveness and appropriateness of the procedures adopted by the Government Communications Security Bureau to ensure compliance with the provisions of **Part 3** of the Government Communications Security Bureau Act **2001** in relation to the issue and

execution of interception warrants and computer access authorisations:".

29 Amendment to New Zealand Security Intelligence Service Act 1969

Section 4J of the New Zealand Security Intelligence Service Act 1969 is amended by repealing subsection (5).

30 Amendment to Official Information Act 1982

The First Schedule of the Official Information Act 1982 is amended by inserting, in its appropriate alphabetical order, the item "Government Communications Security Bureau".

31 Amendment to Public Finance Act 1989

Section 39 of the Public Finance Act 1989, as set out in section 70I of that Act, is amended by repealing subsections (4) and (5), and substituting the following subsection:

"(4) The statement required by subsection (3) must be included in the department's annual report prepared under the New Zealand Security Intelligence Service Act 1969 or the Government Communications Security Bureau Act **2001**, as the case may require."

32 Amendment to Radiocommunications Act 1989

(1) Section 133A(2)(e) of the Radiocommunications Act 1989 is amended by inserting, after subparagraph (ii), the following subparagraph:

"(iia) the Government Communications Security Bureau Act **2001**; or".

(2) Section 133A of the Radiocommunications Act 1989 is amended by repealing subsection (3), and substituting the following subsection:

"(3) For the purposes of this section,—

"(a) **foreign intelligence** has the same meaning as in **section 4** of the Government Communications Security Bureau Act **2001**:

"(b) **security** has the same meaning as in section 2(1) of the New Zealand Security Intelligence Service Act 1969."

New (unanimous)

(3) Section 133A(4) of the Radiocommunications Act 1989 is amended by omitting the words "without an interception warrant and in accordance with that section".

33 Amendments to State Sector Act 1988

(1) Section 44(1) of the State Sector Act 1988 is amended by repealing paragraph (d), and substituting the following paragraphs:

"(d) the Director of the Government Communications Security Bureau; or

"(e) the State Services Commissioner."

(2) Section 44(2) of the State Sector Act 1988 is amended by adding the following paragraph:

"(e) the Director of the Government Communications Security Bureau is the chief executive of the Government Communications Security Bureau."

(3) The First Schedule of the State Sector Act 1988 is amended by inserting, in its appropriate alphabetical order, the item "Government Communications Security Bureau."

34 Certain provisions of State Sector Act 1988 not to apply

Sections 30, 40, 58(2), and 68 of the State Sector Act 1988 do not apply to the Government Communications Security Bureau.

35 Revocation

The Crimes (Exemption of Listening Device) Order 1997 (SR 1997/145) is revoked.

Legislative history

1 May 2001	Introduction (Bill 122-1)
8 May 2001	First reading and referral to Intelligence and Security Committee

Wellington, New Zealand: Published under the authority of the House of Representatives—2001

122bar2.pag
5-NOV-01

Price code: J