No 85

House of Representatives

Supplementary Order Paper

Tuesday, 7 November 2000

Crimes Amendment Bill (No 6)

Proposed amendments

Hon Paul Swain, in Committee, to move the following amendments:

New heading and clauses 16A to 16E inserted
To insert, after *clause 16* (which appears on page 9), the following heading and clauses:

Crimes against personal privacy

16A Interpretation
Section 216A(1) of the principal Act is amended by repealing subsection (1), and substituting the following subsection:

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

"**foreign intelligence** means information relating to the capabilities, intentions, or activities of—
"(a) a foreign organisation; or
"(b) a foreign person

"**foreign organisation** means—
"(a) a government of any country other than New Zealand; or
"(b) an entity controlled by the government of any country other than New Zealand; or
"(c) a company or body corporate that is incorporated outside New Zealand; or
"(d) a 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; or
"(e) an unincorporated body of persons—

"(i) that is not a body, 50% or more of whose members are New Zealand citizens or permanent residents; and

"(ii) that carries on activities wholly or in part outside New Zealand

"**foreign person** means a natural person who is neither—

"(a) a New Zealand citizen; nor

"(b) a person ordinarily resident in New Zealand

"**intercept**, in relation to a private communication, includes hear, listen to, record, monitor, acquire, or receive the communication either—

"(a) while it is taking place; or

"(b) at any time during the period beginning with the time the communication is sent and ending at the time that the intended recipient is able to have access to it

"**interception device**—

"(a) means any electronic, mechanical, or electromagnetic instrument, apparatus, equipment, or other device that is used or is capable of being used to intercept a private communication; but

"(b) does not include—

"(i) a hearing aid or similar device used to correct subnormal hearing of the user to no better than normal hearing; or

"(ii) a device exempted from the provisions of this Part by the Governor-General by Order in Council, either generally, or in such places or circumstances or subject to such other conditions as may be specified in the order

"**private communication**—

"(a) means a communication (whether in oral or written form or otherwise) 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 such 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."

16B Prohibition on use of listening devices

(1) Section 216B of the principal Act is amended by omitting the words "a listening device" in both places where they appear, and substituting in each case the words "an interception device".

(2) Section 216B(3)(b) of the principal Act is amended by omitting the words "the listening device" in both places where they appear, and substituting in each case the words "the interception device".

(3) Section 216B of the principal Act is amended by adding the following subsections:

"(5) Subsection (1) does not apply to the interception of private communications by any interception device operated by the Government Communications Security Bureau for the purpose of intercepting private communications that are both—

"(a) private communications of—

"(i) a foreign organisation, or foreign person; or

"(ii) a representative or agent of a foreign organisation, or foreign person; and

"(b) private communications that contain, or may reasonably be expected to contain, foreign intelligence.

"(6) Subsection (1) does not apply to the interception of private communications by any interception device operated by a person engaged in providing an Internet or other communication service to the public if the interception is carried out—

"(a) by an employee of the person providing the Internet or other communication service to the public in the course of that person's duties; and

"(b) for the purpose of maintaining the Internet or other communication service."

(4) Section 216B of the principal Act is amended by omitting from the heading the words "**listening devices**", and substituting the words "**interception devices**".

16C Prohibition on disclosure of private communication unlawfully intercepted

Section 216C(2)(b)(ii) of the principal Act is amended by omitting the words "a listening device", and substituting the words "an interception device".

16D Prohibition on dealing, etc, with listening devices

Section 216D of the principal Act is amended—

(a) by omitting from subsection (1)(d) the words "any listening device", and substituting the words "any interception device"; and

(b) by omitting from subsection (2)(b) the words "a listening device", and substituting the words "an interception device"; and

(c) by omitting from subsection (2)(b) the words "the listening device" in both places where they appear, and substituting in each case the words "the interception device"; and

(d) by omitting from the heading the words "**listening devices**", and substituting the words "**interception devices**".

16E Forfeiture

Section 216E of the principal Act is amended by omitting the words "listening device" wherever they appear, and substituting in each case the words "interception device".

Clause 19

To add to *new section 305ZD* (after line 39 on page 23) the following definitions:

"**foreign intelligence** has the same meaning as in section 216A(1)

"**foreign organisation** has the same meaning as in section 216A(1)

"**foreign person** has the same meaning as in section 216A(1).

To insert, after *new section 305ZF* (after line 32 on page 24), the following sections:

"305ZFA **Accessing computer system without authorisation**

"(1) Every one is liable to imprisonment for a term not exceeding 2 years who intentionally accesses, directly or indirectly, any computer system or part of a computer system without authorisation knowing that he or she is not authorised to access that computer system or part of that computer system or being reckless as to whether or not he or she is authorised to access that computer system or part of that computer system.

"(2) To avoid doubt, **subsection (1)** does not apply if a person is authorised to access a computer system or part of a computer system for a specified purpose or purposes but accesses it for some other purpose or purposes.

"305ZFB **Qualified exemption to access without authorisation offence for New Zealand Security Intelligence Service**

Section 305ZFA does not apply if—

"(a) the person accessing a computer system or part of a computer system is—

"(i) the person specified in an interception warrant issued under the New Zealand Security Intelligence Service Act 1969; or

"(ii) a person, or member of a class of persons, requested to give any assistance that is specified in that warrant; and

"(b) the person accessing a computer system or part of a computer system is doing so for the purpose of intercepting or seizing any communication, document, or thing of the kind specified in that warrant.

"305ZFC **Qualified exemption to access without authorisation offence for Government Communications Security Bureau**

"(1) **Section 305ZFA** does not apply if the person accessing a computer system or part of a computer system—

"(a) is an employee of the Government Communications Security Bureau; and

"(b) is discharging his or her duty as an employee of the Government Communications Security Bureau to collect foreign intelligence; and

"(c) is authorised, in writing, by the Minister responsible for the Government Communications Security Bureau.

"(2) The Minister responsible for the Government Communications Security Bureau may authorise an employee of the Government Communications Security Bureau to access a computer system or part of a computer system of a specified foreign organisation or foreign person if the Minister—

"(a) has consulted with the Minister of Foreign Affairs and Trade; and

"(b) is satisfied that—

"(i) there are reasonable grounds to believe that no New Zealand citizen or person ordinarily resident in New Zealand is specified as a foreign organisation or foreign person whose computer system may be accessed; and

"(ii) the access is necessary for the purposes of collecting foreign intelligence; and

"(iii) the value of the information sought to be obtained justifies the access; and

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

"305ZFD **Qualified exemption to access without authorisation offence for law enforcement agencies**

To avoid doubt, if access to a computer system or part of a computer system is gained under the execution of an interception warrant, search warrant, or other legal authority, such access does not constitute an offence under **section 305ZFA**.

Heading above clause 20

To omit the heading immediately above *clause 20* on page 30, and substitute the following heading:

Other amendments to principal Act

New clause 20A

To insert, after *clause 20* (which appears on page 30), the following clause:

20A Heading to Part XIA amended

The heading to Part XIA of the principal Act is amended by omitting the words "**listening devices**", and substituting the words "**interception devices**".

Clause 21

To omit this clause (which appears on pages 30 and 31), and substitute the following clauses:

21 Interpretation

(1) Section 312A(1) of the principal Act is amended by repealing the definitions of **intercept** and **private communication**, and substituting, respectively, the following definitions:

"**intercept**, in relation to a private communication, includes hear, listen to, record, monitor, acquire, or receive the communication either—

"(a) while it is taking place; or

"(b) at any time during the period beginning with the time the communication is sent and ending at the time that the intended recipient is able to have access to it

"**private communication**—

"(a) means a communication (whether in oral or written form or otherwise) 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 such 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".

(2) Section 312A(1) of the principal Act is amended by repealing the definition of **listening device**.

(3) Section 312A(1) of the principal Act is amended by inserting, in its appropriate alphabetical order, the following definition:

"**interception device**—

"(a) means any electronic, mechanical, or electromagnetic instrument, apparatus, equipment or other device that is used or is capable of being used to intercept a private communication; but

"(b) does not include a hearing aid or similar device used to correct subnormal hearing of the user to no better than normal hearing".

(4) Section 312A(1) of the principal Act is amended by repealing paragraphs (d) to (f) of the definition of **specified offence**, and substituting the following paragraphs:

"(d) an offence punishable under **section 305G(b)** (theft of an object exceeding $1,000 in value):

"(e) an offence against **section 305Y** (which relates to money laundering):

"(f) an offence punishable under **section 305ZC(a)** (which relates to receiving property dishonestly obtained)."

21A Application by Police for warrant to intercept private communications

(1) Section 312B(1) of the principal Act is amended by omitting the words "a listening device", and substituting the words "an interception device".

(2) Sections 312B(2) of the principal Act is amended by repealing paragraph (c), and substituting the following paragraph:

(c) the name and address, if known, of the suspect whose private communications there are reasonable grounds for believing will assist the police investigation of the case, or, if the name and address of the suspect are not known, a general description of the premises, place, thing, or facility in respect of which it is proposed to intercept private communications, being premises or a place, thing, or facility believed to be used for any purpose by any member of the organised criminal enterprise; and".

21B Matters on which Judge must be satisfied in respect of applications

Section 312C(1)(b) of the principal Act is amended by omitting the words "a listening device", and substituting the words "an interception device".

21C Application by Police for warrant to intercept private communications in relation to serious violent offences

(1) Section 312CA of the principal Act is amended by omitting the words "a listening device" wherever they appear, and substituting in each case the words "an interception device".

(2) Section 312CA(2)(c) is amended by repealing subparagraph (ii), and substituting the following subparagraph:

(ii) if the name and address of the suspect are not known, a general description of the premises, place, thing, or facility in respect of which it is proposed to intercept private communications, being premises or a place, thing, or facility believed to be used for any purpose by any person—

(A) whom it is believed has committed, or is committing, or is about to commit, a serious violent offence; or

(B) whom it is believed was involved, or is involved, or will be involved, in the commission of a serious violent offence; and".

21D Matters on which Judge must be satisfied in respect of applications relating to serious violent offences

Section 312CB of the principal Act is amended by omitting the words "a listening device" wherever they appear, and substituting in each case the words "an interception device".

21E Contents and term of warrant

(1) Section 312D of the principal Act is amended by omitting the words "a listening device" in both places where they appear, and substituting in each case the words "an interception device".

(2) Section 312D(1) of the principal Act is amended by repealing paragraph (b), and substituting the following paragraph:

(b) state,—

(i) in the case of a warrant granted under section 312C, the name and address of the suspect, if known, whose private communications may be intercepted, or, where the suspect's name and address are not known, the premises, place, thing, or facility believed to be used for any purpose by any member of the organised criminal enterprise; or

(ii) in the case of a warrant granted under section 312CB, the name and address of the suspect, if known, whose private communications may be intercepted, or, where the suspect's name and address are not known, the premises, place, thing, or facility in respect of which private communications may be intercepted, being premises or a place, thing, or facility believed to be used for any purpose by any person—

(A) whom it is believed has committed, or is committing, or is about to commit, a serious violent offence; or

(B) whom it is believed was involved, or is involved, or will be involved, in the commission of a serious violent offence; and".

21F Effect of warrant

Section 312E of the principal Act is amended by omitting the words "a listening device", and substituting the words "an interception device".

21G Emergency permits
Section 312G of the principal Act is amended by inserting, after the words "a particular place", the words "or a particular thing or a particular facility".

21H Destruction of irrelevant records made by use of listening device
Section 312I of the principal Act is amended by omitting from the heading the words "**listening device**", and substituting the words "**interception device**".

21I Destruction of relevant records made by use of listening device
Section 312J of the principal Act is amended by omitting from the heading the words "**listening device**", and substituting the words "**interception device**".

21J Notice to be given of intention to produce evidence of private communication
Section 312L(b) of the principal Act is amended by inserting, after the word "place", the words "(if known)".

21K Inadmissibility of evidence of private communications unlawfully intercepted
Section 312M of the principal Act is amended by omitting the words "a listening device" wherever they appear, and substituting in each case the words "an interception device".

21L Report to be made to Judge on use of warrant or permit
Section 312P of the principal Act is amended by omitting the words "listening device" wherever they appear, and substituting in each case the words "interception device".

21M Commissioner of Police to give information to Parliament
Section 312Q of the principal Act is amended by omitting from paragraph (f) the words "a listening device" in both places where they appear, and substituting in each case the words "an interception device".

Clause 27
To add, as subsection (2), the following subclause:

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

New heading and clause 29
To insert, after *clause 28* (which appears on page 33), the following heading and clause:

Interception devices

29 Amendments to enactments relating to interception devices

The enactments specified in **Schedule 3** are amended in the manner included in that schedule.

New Schedule 3

To add the following schedule:

Schedule 3 s 29
Acts relating to listening devices amended

Evidence Act 1908 (1908 No 56)

Omit from the heading to section 23B the words "**listening device**" and substitute the words "**interception device**".

Omit from section 23B(1) the words "a listening device" and substitute the words "an interception device".

International Terrorism (Emergency Powers) Act 1987 (1987 No 179)

Repeal the definitions of **intercept** and **private communication** in section 2(1) and substitute, respectively:

"**intercept**, in relation to a private communication, includes hear, listen to, record, monitor, acquire, or receive the communication either—

"(a) while it is taking place; or

"(b) at any time during the period beginning with the time the communication is sent and ending at the time that the intended recipient is able to have access to it

"**private communication**—

"(a) means a communication (whether in oral or written form or otherwise) 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 such 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".

Omit from section 10(3)(a) the word "telephone" and substitute the word "telecommunications".

Omit from section 10(3)(b) the word "telephonic".

Misuse of Drugs Amendment Act 1978 (1978 No 65)

Repeal the definitions of **intercept** and **private communication** in section 10(1) and substitute, respectively:

"**intercept**, in relation to a private communication, includes hear, listen to, record, monitor, acquire or receive the communication either—

Misuse of Drugs Amendment Act 1978 (1978 No 65)—continued

"(a) while it is taking place; or

"(b) at any time during the period beginning with the time the communication is sent and ending at the time that the intended recipient is able to have access to it

"**private communication**—

"(a) means a communication (whether in oral or written form or otherwise) 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 such 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".

Repeal the definition of **listening device** in section 10(1).

Insert in section 10(1), in its appropriate alphabetical order:

"**interception device**—

"(a) means any electronic, mechanical, or electromagnetic instrument, apparatus, equipment, or other device that is used or is capable of being used to intercept a private communication; but

"(b) does not include a hearing aid or similar device used to correct subnormal hearing of the user to no better than normal hearing".

Omit from sections 10(1), 14(1), 15(1)(b), 15A(1), 15B(1)(b), 16(1)(d) and (2), 17, 25(1) and (4), 28(3) and (4), and 29 the words "a listening device" wherever they appear and substitute in each case the words "an interception device".

Repeal section 14(2)(c) and substitute:

"(c) the name and address, if known, of the suspect whose private communications there are reasonable grounds for believing will assist the police investigation of the case, or, if the name and address of the suspect are not known, a general description of the premises, place, thing, or facility in respect of which it is proposed to intercept private communications, being premises or a place, thing, or facility believed to be used for any purpose by any person involved in the drug dealing offence; and".

Repeal section 15A(2)(c) and substitute:

"(c) the name and address, if known, of the suspect whose private communications there are reasonable grounds for believing will assist the police investigation of the case, or, if the name and address of the suspect are not known, a general description of the premises, place,

Misuse of Drugs Amendment Act 1978 (1978 No 65)—continued

thing, or facility in respect of which it is proposed to intercept private communications, being premises or a place, thing, or facility believed to be used for any purpose by any member of the organised criminal enterprise; and".

Repeal section 16(1)(b) and substitute:

"(b) state,—

"(i) in the case of a warrant granted under section 15, the name and address of the suspect, if known, whose private communications may be intercepted, or, where the suspect's name and address are not known, the premises, place, thing, or facility in respect of which private communications may be intercepted, being premises or a place, thing, or facility believed to be used for any purpose by any person involved in the drug dealing offence; or

"(ii) in the case of a warrant granted under section 15B, the name and address of the suspect, if known, whose private communications may be intercepted, or, where the suspect's name and address are not known, the premises, place, thing, or facility in respect of which private communications may be intercepted, being premises or a place, thing, or facility believed to be used for any purpose by any member of the organised criminal enterprise; and".

Insert in section 19(1), after the words "a particular place", the words "or a particular thing or a particular facility".

Omit from the headings to sections 21 and 22 the words "**listening device**" and substitute in each case the words "**interception device**".

Insert in section 24(b), after the word "place", the words "(if known)".

Police Act 1958 (1958 No 109)

Omit from section 65(3) the words "a listening device" and substitute the words "an interception device".

Telecommunications Act 1987 (1987 No 116)

Omit from section 10(1) the words "a listening device" and substitute the words "an interception device".

Explanatory note

This Supplementary Order Paper adds a new computer offence to those currently included in the Crimes Amendment Bill (No 6), amends the existing interception offences in Part IXA of the Crimes Act 1961 (the principal Act), amends the police interception warrant regime contained in Part XIA of the principal Act and Part II of the Misuse of Drugs Amendment Act 1978, and makes related changes to other enactments.

The new computer offence (*new section 305ZFA*) is the offence of accessing a computer system without authorisation. It will be an offence, punishable by a maximum term of 2 years' imprisonment, for a person to intentionally access a computer system or part of a computer system without authorisation, knowing that he or she is not authorised to do so, or being reckless as to whether he or she is authorised to do so. This conduct is commonly referred to as computer "hacking".

The rationale for this offence is the need to protect the security of computer systems. The proposed computer offences currently included in the Crimes Amendment Bill (No 6) cover more serious conduct, such as that which results in gain, loss, or damage. The new offence included in this Supplementary Order Paper relates to unauthorised access where none of these things occurs. The creation of a new offence is justified because, even if no loss or damage occurs, "hacking" may force owners of computer systems who become aware of a hacker's activities to engage in expensive and time-consuming efforts to check whether any damage has been done. The new offence will cover employees who are not authorised to access a particular part of their employer's computer system, as well as "hackers" from outside the organisation.

Certain qualified exemptions to the new offence are proposed for—

- the New Zealand Security Intelligence Service (*new section 305ZFB*):
- the Government Communications Security Bureau (*new section 305ZFC*):
- law enforcement agencies (*new section 305ZFD*).

Employees of the New Zealand Security Intelligence Service will only be exempt if acting under an interception warrant obtained under the New Zealand Security Intelligence Service Act 1969. Employees of the Government Communications Security Bureau will only be exempt if acting under an authorisation from the Minister responsible for the Government Communications Security Bureau (a similar procedure to the interception warrant procedure provided in the New Zealand Security Intelligence Service Act 1969). Without such exemptions, the ability of the security agencies to obtain information would be limited and this would compromise them in the performance of their functions.

Currently, the police and other law enforcement agencies have various powers of search or inspection that authorise searching a computer. The purpose of the exemption for law enforcement agencies is to ensure that the offence (once enacted) does not prevent those law enforcement agencies from carrying out their lawful activities.

Interception

The interception offence in section 216B of the principal Act applies only to private oral communications. The Supplementary Order Paper extends the definition of **private communication** to other forms of private communication that can be intercepted by means of an interception device, such as e-mail, faxes, and message pagers. The main justification for the change is that all forms of private communication should have the same level of protection, where there is a reasonable expectation of privacy. (The extension of the definition of **private communication** involves other related amendments, such as changing the term **listening device** to **interception device**.)

Currently, the offence in section 216B of the principal Act does not apply to the following people or agencies:

- a person who is a party to the communication:
- telecommunications employees, to whom the exemption contained in the Telecommunications Act 1987 applies, engaged in network maintenance:
- the New Zealand Security Intelligence Service, when authorised under the New Zealand Security Intelligence Service Act 1969:
- the police, when authorised, or in an emergency if life or serious injury may be at risk:
- the prison service, if monitoring inmate phone calls under the Penal Institutions Act 1954:
- the Government Communications Security Bureau's Waihopai site (which is exempted by an Order in Council).

The Supplementary Order Paper also exempts from the offence in section 216B of the principal Act interception by employees of Internet or other communication service providers to the public for the purpose of maintaining the system. This is similar to the exemption for telecommunication network operators under the Telecommunications Act 1987. The additional exemption is considered necessary as not all public communication service providers are network operators under that Act.

In addition, the exemption for the Government Communications Security Bureau's Waihopai site, which is in the Crimes (Exemption of Listening Device) Order 1997 (SR 1997/145), is moved (in a modified form) into the principal Act (*new section 216B(5)*). The exemption will now extend to any interception device operated by the Bureau for the purpose of obtaining foreign intelligence.

The same amendments proposed to the definitions in Part IXA of the principal Act are also proposed to the definitions applicable to police interception warrants (Part XIA of the principal Act). Amending the definition of **private communication** will allow the police to obtain an interception warrant to intercept e-mails, faxes, etc. If the police obtain an interception warrant under Part XIA of the principal Act, it will now be lawful for the police to access that person's electronic as well as oral communications. The existing preconditions

that must be satisfied before a interception warrant is granted will continue to apply.

Wellington, New Zealand: Published under the authority of the
House of Representatives—2000

3309SV8.pag
6-NOV-00