Crimes against personal privacy and crimes involving computers: Intercepting private communications and accessing computer systems without authorisation

Report by the Privacy Commissioner to the Minister of Justice on Supplementary Order Paper No 85 to the Crimes Amendment Bill (No 6)

13 December 2000

Privacy Commissioner
Te Mana Matapono Matatapu
EXECUTIVE SUMMARY

This report sets out the results of the Privacy Commissioner’s examination of proposed amendments to the Crimes Act 1961. Supplementary Order Paper 85 makes two principal amendments to the Crimes Act which the Commissioner supports:

- broadening “crimes against personal privacy” by including the interception of non-oral private communications within the prohibition against intercepting private communications;
- creating a new offence of accessing a computer system without authorisation.

The expansion of laws against unauthorised interception of private communications to encompass communications such as faxes is an overdue and welcome reform. Similarly the criminalising of hacking into computers is beneficial to privacy. However, the bill does not simply criminalise such actions. It also provides exemptions and authorisations for state intrusions of the same type. This represents a significant risk to privacy and the Commissioner’s recommendations seek to limit state intrusion and promote appropriate control and accountability when such intrusions are warranted.

Principal recommendations include:

- ensuring that new exemptions to the interception law cannot be made by delegated legislation;
- subjecting Internet service providers and telecommunications network operators to criminal sanctions if they retain, use or disclose private communications obtained during maintenance work;
- delaying exemptions from the new laws for the Government Communication Security Bureau until it is placed on a statutory footing and is subject to an interception warrant process;
- opposing the pernicious practice of police hacking into computer databases;
- calling for full and meaningful public reporting of any state practices involving intercepting non-oral communications and accessing computer systems.
1. INTRODUCTION

1.1 The Crimes Amendment Bill (No 6) inserts into the Crimes Act 1961 a variety of new crimes involving computers. I earlier welcomed the provisions criminalising accessing computer systems for dishonest purposes and damaging or interfering with computer systems but noted that the legislative scheme was incomplete. The bill omitted to criminalise the unauthorised accessing of computers (in some contexts called “hacking”) regardless of whether any property damage is done or the offender has a dishonest purpose.

1.2 Supplementary Order Paper No 85 addresses the omission by:
   • amending the provisions concerning “crimes against personal privacy” by including the interception of non-oral private communications within the prohibition against intercepting private communications;
   • creating a new offence of accessing a computer system without authorisation within the “crimes involving computers”.

1.3 I support the creation of the new offence provisions. The expansion of laws against unauthorised interception of private communications to encompass communications such as faxes is an overdue and welcome reform. Similarly it is high time that hacking into computers was criminalised.

1.4 However, the bill does not simply criminalise such interceptions of communications and accessing of computers. It also provides exemptions and authorisations for state intrusions of the same type. This represents a risk to privacy. In this report I make a number of recommendations to more appropriately limit state intrusion and promote appropriate control and accountability when such intrusions are warranted.

2. OVERVIEW

2.1 The amendments both enhance and intrude into privacy:
   • they enhance privacy protections through the use of the criminal law, by outlawing interception of a range of non-oral private communications and the unauthorised accessing of computer systems; and
   • they expressly limit those privacy protections, both in terms of the scope of the offence provisions themselves and by creating exemptions - indeed, many people may see the greater significance of the measure as being the...
authorisation of intrusions into privacy rather than offering protections against such intrusions.

2.2 Consistent with the previous stance I have taken, I start from the position of supporting the proposals to:

- prohibit the interception of non-oral private communications; and
- outlaw the unauthorised access to computer systems.²

2.3 Although I have misgivings about some of the exemptions, I do, in principle, accept a case for some appropriately crafted exceptions to the new laws to enable law enforcement agencies, intelligence agencies and service providers, to continue the activities that they are currently quite lawfully carrying out. In accepting a case for some appropriate exemptions to the new laws I am bound to note that privacy often needs to be balanced against other competing public interests and the exemptions are one way of achieving this.³ Nor am I accepting a case for any major expansion of State surveillance. Rather, the exemptions should principally allow the continuation of existing practice.

2.4 Accepting the need to take account of competing public interest does not mean that those interests should in every case overwhelm the public interest in protecting the privacy of its citizens. Any free and democratic society must reasonably respect the right of individuals to communicate in private. In the 21st century the confidence that one’s computer system is secure from intrusion - so far as the law can ever achieve that - is an essential feature of private life and the ability freely to communicate.

2.5 It is easy to think of the interception of communications or the accessing of a computer as affecting only the target of Police interest. However, the interception warrant system is not to protect only that person. Also of importance are the many other people affected by interceptions or computer related searches. Trawling or browsing through a myriad of personal information is being authorised in an unprecedented scale. A single interception warrant can, for instance, involve authorised listening into hundreds of conversations involving scores of individuals beyond the targeted individuals.⁴

2.6 I have scrutinised the supplementary order paper given that the proposed amendments to the Crimes Act and other laws may affect individual privacy in a beneficial or adverse way. I draw to your attention a number of clauses which raise matters of concern. In all cases, I make recommendations for amendment which may better clarify the law or may, in my opinion, strike a more appropriate balance between collective rights to privacy and competing state interests.

⁴ See para 4.11 below.
Over recent years I have examined a number of bills which deal with the interception of private communications and the powers of intelligence agencies. Typically these have involved the expansion of the powers of law enforcement and intelligence agencies to carry out covert investigations. However, I am pleased to note a willingness in this and previous governments to occasionally enhance accountability and oversight arrangements.

At the end of the report, I reflect on some aspects of our current legal arrangements governing interception of private communications and make further recommendations for reform. This latter “unfinished business” part of the report builds upon a series of earlier recommendations which I believe should be implemented. Although it may not be possible or appropriate for all such matters to be taken up in this bill, I do hope that they may be given consideration before another piece of legislation to expand the infrastructure of covert investigative powers.

3. CLAUSE BY CLAUSE COMMENT

CRIMES AGAINST PERSONAL PRIVACY

3.1 Section 216A(1) — Definition of “interception device” (clause 16B)

3.1.1 This clause includes two key definitions used throughout Part IXA of the Crimes Act. These are:

"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."

See para 4.4 below.

For example through the establishment of the Inspector General of Intelligence and Security in 1996.
3.1.2 To reflect the expansion of authorised interception beyond eavesdropping to include other types of interception and surveillance of non-oral private communications, the clause replaces the existing definition of “listening device” by a similar definition of “interception device”. The definitions are virtually identical with some modest reformatting to make them consistent with current drafting style. However, “private communication”, is a component of the definition of “interception device”, and therefore the meaning is widened to include devices which intercept non-oral communications. Accordingly, the new definition will not only cover hidden microphones and other devices used for bugging premises or tapping telephones, but also equipment used for intercepting email, fax, pager messages, sign language and other non-oral communication.

3.1.3 I draw attention to the exception to “interception device” found in subparagraph (b)(ii). This continues current provision in the definition of “listening device” for exemption by Order in Council. The Crimes (Exemption of Listening Device) Order 1997 made under this provision exempted the substantial Defence Satellite Communications Unit facility operated by the Government Communications Security Bureau (GCSB) in Marlborough (Waihopai). It surprised many people to see the Order in Council power used to legitimise such a major operation. It is therefore to be welcomed that that exemption is now being transferred into primary legislation. It is my view that the entire operation of GCSB should be placed on a proper statutory footing so that Parliament can be truly said to authorise and control its operation rather than it simply being an Executive matter.

3.1.4 Given that the Order in Council process has only been used on the one occasion, with this bill implicitly acknowledging that even that exemption should have been located in primary legislation, I question whether the Order in Council process should be continued. My preference would be for the Order power to be dropped, with any new exemptions being made by statutory amendment with full Parliamentary scrutiny. However, if the flexibility of the exemption process is to be retained, I suggest that there ought to be some guidance as to the purposes for which an Order may be made and some additional Parliamentary scrutiny.

3.1.5 A principal purpose for having an exemption power would seem to be to exclude equipment which, although it might appear to have the characteristics of an “interception device”, should not be subject to the regime. The obvious example is the one included in the statute itself: a hearing aid. Had there been no statutory exemption for hearing aids, it would have been uncontroversial to exempt them by Order. However, the Order process should not again be used for exempting an entire State agency’s interception activities from the law by deeming that agency’s powerful devices to be exempt. An exemption of that type ought only to be allowed if explicitly established in statute.

---

7 See proposed new section 305ZFC. However, as I note below there is one feature of that 1997 Order which is not carried over in the new exemption.
3.1.6 My second suggestion is that any Orders given under the section be confirmed by a Parliamentary vote within, say, 12 months. There are a number of examples of statutes which provide for the making of regulations which must be confirmed by Act of Parliament. The opportunity for Parliamentary scrutiny and public submission could be accommodated through the annual Subordinate Legislation (Confirmation and Validation) Bill. If a more rapid Parliamentary process was desired, it would be possible for the confirmation process to be done by resolution of the House but there are apparently no precedents for such a procedure.

3.1.7 Accordingly, I recommend that the provision for exempting devices from the provisions of Part IXA of the Crimes Act by Order in Council be dropped. However, if the exemption power is to be retained I recommend that:
(a) the purpose for granting such exemptions be made explicit and limited; and
(b) such Orders be subject to a sunset clause at the expiry of which they must have been confirmed by Parliament or expire.

3.2 Section 216B(5) and (6) — Exemptions from prohibition on use of listening devices (clause 16B)

3.2.1 Section 216B establishes the offence of using a listening device to intercept a private communication. It is subject to several existing statutory exceptions and clause 16B establishes two new exemptions relating to:
• the Government Communications Security Bureau; and
• employees of Internet or other communication service providers.

Government Communications Security Bureau

3.2.2 It is proposed that a new subsection (5) be inserted as follows:

"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."

3.2.3 Definitions of "foreign intelligence", "foreign organisation" and "foreign person", each of which are used in this subsection, are to be inserted into the

---

Act. I have two principal concerns at granting GCSB this exemption. First, although the Bureau is an important government intelligence agency it is not established by any statute. This lack of a statutory basis means that Parliament has had little say as to the constitution and activities of the agency and Parliament and the public has no real way of knowing precisely who GCSB is or what it does. If GCSB were to completely change the character of its activities next week, the public and Parliament would be unaware of whether it was continuing to fulfil a function for which an exemption from the criminal law is warranted. Placing GCSB on a statutory basis would bring benefits in terms of certainty, transparency and accountability depending upon how the statute were to be written. I accordingly welcome the Government’s recent public confirmation that the Bureau is to get its own statute.

3.2.4 My second principal cause for concern is that, unlike the NZ Security Intelligence Service (NZSIS), any interceptions which may be carried out are not subject to a statutory warrant process. Statutory warrants are one of the few means that free and democratic societies have devised for authorising and constraining especially intrusive investigative techniques. This will not be put right until GCSB's establishment is confirmed and set out in legislation.

3.2.5 A precursor to GCSB having the benefit of an exemption from the prohibition on the use of listening devices, should be to:
- place the Bureau on a statutory footing; and
- create a statutory warrant process for the Bureau to undertake any intrusive activity particularly where that activity would, if performed by any other person, constitute a breach of the law.
Noting the announcement in early December that it is the Government’s intention to introduce a GCSB bill, I suggest that it would be valuable to have that bill available publicly by the time public submissions must be made on the present measure.

3.2.6 It is acknowledged that although subsection (5) will constitute a new statutory exemption, GCSB has had the benefit since 1997 of an exemption pursuant to the Crimes (Exemption of Listening Device) Order 1997. The 1997 Order was in similar terms to the new statutory exemption but it was limited to the Bureau’s Waihopai site. The new exemption is not limited to one place and therefore if the statutory exemption is granted there is nothing to stop GCSB from relocating its apparatus or expanding its interception operations to other locations. Given the very limited information that is currently made publicly available about the activities of GCSB, the loss of information which might signal significant changes in the Bureau’s operations might be seen as regrettable.11

---

10 See clause 16A. The definitions are consistent with those in recent amendments to the New Zealand Security Intelligence Act 1969 (NZSIS Act), section 2, Radiocommunications Act 1989, section 133A, and as found in the Crimes (Exemption of Listening Device) Order 1997, clause 2.

11 This is a case in which the placing of GCSB on a statutory basis will bring benefits; it will be possible to require GCSB to file annual reports giving pertinent information rather than the very limited information gleaned from an occasional exemption Order.
3.2.7 Moving the exemption from an Order in Council to a statute need not necessarily mean that information about the location of GCSB devices must be dispensed with. The same information could be included in the statute (meaning that any expansion or relocation of its activities would require an amendment to the Act). Alternatively, the statutory exemption could remain but with a proviso that it applies only to interception based at any location specified in an Order. This would mean that the basic exemption offers the certainty and high constitutional status of primary legislation while the detail of the location of any satellite station remains on the public record but is notified, if changed, by statutory instrument.

3.2.8 Accordingly, I recommend that the GCSB exemption either:
(a) state the place from which interception may be carried out; or
(b) state that interception may be carried out only from a place described in an Order in Council.

**Internet service providers etc**

3.2.9 A second new exemption relating to ISPs and other communication service providers is to be provided. The proposed subsection (6) states:

"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."

3.2.10 This exemption is similar to that provided for network operators under the Telecommunications Act 1987. Section 10 of that Act provides:

"Monitoring of telecommunications
Any employee of a network operator may, when acting in the course of, and for the purposes of, his or her duty, intercept any telecommunication by means of a listening device or other device for the purposes of maintaining telecommunication services."

3.2.11 I question whether there really is a need for ISPs to have access to the content of personal communications. Such an exemption should not be lightly given and the Government and Parliament should satisfy itself, through expert evidence, that such access indeed is necessary. However, assuming such access to be necessary, there should be further statutory control in the scheme of the Crimes Act on the actions of those exempted from this law.

3.2.12 I consider that Part IXA of the Crimes Act ought to provide that:
- any information obtained by the persons benefiting from the exemption must only be used for the purpose of maintaining the Internet or other communication service;
- such information must not be disclosed to anyone, other than the persons concerned, except where required by law, and
- such information must be promptly destroyed when no longer needed for the purpose of maintaining the Internet or other communication service.

This should be accompanied by an offence provision. There should be similar obligations on persons benefiting from the exemption contained in section 216(2)(b)(ii) as well (that is, network operators under the Telecommunications Act).

3.2.13 I also recommend that a new paragraph (c) should be added to emphasise that accessing the content of messages should only occur where there is no practical alternative. The new paragraph could state:

"and
(c) the interception is essential for that purpose."

This will ensure that interception of private communications for the purpose of maintaining and Internet or other communication service is only permissible when it is the only way of maintaining the service and not merely a convenient or possible way of doing so.

CRIMES INVOLVING COMPUTERS

3.3 New section 305ZFA - Accessing computer system without authorisation (clause 19)

3.3.1 The proposed new section 305ZFA states:

"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

---

12 See Electronic Communications Privacy Act 1986 (USA), §2511(3).
13 Section 133A of the Radiocommunications Act 1989 may offer a suitable precedent ("offence to disclose contents of radiocommunications").
14 There are criminal sanctions in Australian interception law for telecommunications network operators which use or disclose personal information obtained through interception for network maintenance purposes: see Telecommunications (Interception) Act 1979 (Cth).
15 Laws in other jurisdictions sometimes address this issue. For example, in the United States there is a qualified exemption in §2511(2)(a)(i) of the Electronic Communications Privacy Act 1986 for employees of providers of wire or electronic communication services where intercepting or using communications "in the normal course of ... employment while engaged in any activity which is a necessary incident to the rendition of ... service or to the protections of the rights or property of the provider of that service." That exemption is further qualified by stating that a provider to the public "shall not utilise service observing or random monitoring except for mechanical or service quality control checks".
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.

"(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."

3.3.2 As can be seen, this provision creates an offence for a person to intentionally access a computer system or part of a system without authorisation, knowing that he or she is not authorised to do so, or being reckless as to whether he or she is so authorised. This is an important addition to New Zealand's computer crime laws. I support its enactment as it has the potential to deter and punish actions which can do significant harm to privacy.

3.3.3 The explanatory note mentions that the conduct being criminalised is commonly referred to as computer "hacking". Certainly hacking is a major component of the proscribed behaviour. However, it is misleading to think this is all that is covered. The archetypal hacker is an outsider who may steal or guess a password, or bypass inadequate security controls, and enter a government or business system through the Internet. However, the offence will also apply to insiders, such as employees, who access computer systems without authorisation.

3.3.4 It is in this latter respect that the drafting of subclause (2) may be confusing. The intended effect is as described in the explanatory note: 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. While this is clearly stated in the explanatory note, and is indeed the correct interpretation of the words of the section as drafted, I suggest that subclause (2) may confuse people into thinking the opposite.

3.3.5 It may be useful to use an example. A payroll system forms part of a company's computer system but only staff in the personnel department are authorised to access it. Employee A is not in the personnel department but, knowing she is not authorised to do so, obtains a payroll clerk's password and accesses the system to check her co-workers' salary details. Employee A will likely have breached the section. Employee B, on the other hand, works in the personnel department and is authorised to access the payroll system as part of his duties to make fortnightly payments. However, outside his duties employee B also checks his co-workers' salary details. Employee B will not have breached the section.\(^{16}\)

\(^{16}\) Notwithstanding employee B has not breached section 305ZFA, his actions would likely have employment law consequences for such misconduct. If employee B were to use his privileged access to pass or sell information to, say, a debt collector he may have committed other crimes. For example, he may have breached section 305ZB ("accessing computer system for dishonest purpose") and, if the employer was a government agency, 105A of the Crimes Act ("corrupt use of official information"). The debt collector may be in breach of section 105B ("use or disclosure of personal information disclosed in breach of section 105A").
3.3.6 I accept that this is an appropriate outcome. However, it may be worthwhile to consider whether the drafting can be improved to make the intention plainer (especially if the select committee finds confusion amongst people making submissions on this clause).

3.4 New section 305ZFC - Qualified exemption to access without authorisation offence for Government Communication Security Bureau (clause 19)¹⁷

3.4.1 This clause gives an exemption to employees of GCSB allowing them to access computer systems without authorisation where the employees are:
- discharging their duties as employees of the Government Communication Security Bureau to collect foreign intelligence; and
- they are authorised, in writing, by the Minister responsible for GCSB.¹⁸

3.4.2 The section goes on to set out criteria for the Minister to authorise GCSB employees to access computer systems or parts of computer systems. The criteria are that the Minister has consulted with the Minister of Foreign Affairs and Trade and is satisfied that:
- there are reasonable grounds to believe no New Zealand citizen or person ordinarily resident in New Zealand is specified as a foreign organisation or a foreign person whose computer system may be accessed; and
- the access is necessary for the purposes of collecting foreign intelligence; and
- the value of the information sought to be obtained justifies the access; and
- the information is not likely to be obtained by other means.¹⁹

3.4.3 I have already expressed the opinion that exemptions of this nature should not be granted to a body which is not established under statute and therefore lacks the desirable features of:
- high-level Parliamentary authorisation;
- transparency as to the nature of its mandate and the limits on its activities;
- detailed legal controls on covert and intrusive activities.

3.4.4 As also noted, the establishment of GCSB on a statutory basis can bring to bear other desirable accountabilities such as the obligation to prepare an annual report to be made available to Parliament and the public.

3.4.5 My further concern is that the written authorisation contemplated by the section is inferior to a full statutory warrant process. Contrast the position with that of

¹⁷ This and the following section heading may confuse. Might “Qualified exemption to section 305ZFA offence for Government Communications Security Bureau” be better?
¹⁸ Section 305ZFC(1).
¹⁹ Section 305ZFC(2).
the NZSIS. The following provisions are absent from written authorisations for GCSB but were present in warrants issued under the New Zealand Security Intelligence Service Act 1969:

- a limited statutory term for each authorised interception;\(^{20}\)
- duty to minimise impact of interception warrants on third parties;\(^{21}\)
- destruction of irrelevant records obtained by interception;\(^{22}\)
- public reporting on warrants;\(^{23}\)
- joint issue of warrants by a Minister and a judicial officer.\(^{24}\)

3.4.6 Accordingly, I recommend that an exemption for GCSB should not take effect until:

(a) the Bureau is placed on a statutory footing;\(^{25}\) and

(b) an interception warrant process is in place with appropriate safeguards, going beyond simply the criteria that the responsible Minister is to apply in approving accessing of computer systems.

3.5 New section 305ZFD — Qualified exemption to access without authorisation offence for law enforcement agencies (clause 19D)\(^{26}\)

3.5.1 Proposed section 305ZFD provides as follows:

"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."

I have substantial reservations about this section.

3.5.2 The first is that although the heading refers to the exemption being “for law enforcement agencies”, the text of the clause itself does not. This is not a problem in relation to execution of an interception warrant or search warrant, since both are granted only to law enforcement agencies. However, the meaning of “other legal authority” is unclear (a point to which I return below) and would not necessarily be limited to authority possessed by law enforcement agencies. I recommend that the clause explicitly state that it is an exemption only available

\(^{20}\) NZSIS Act, section 4C.
\(^{21}\) NZSIS Act, section 4F.
\(^{22}\) NZSIS Act, section 4G.
\(^{23}\) NZSIS Act, section 4J.
\(^{24}\) NZSIS Act, section 4A. The judicial officer is the Commissioner of Security Warrants: NZSIS Act, sections 5A-5G. However, note that the Commissioner of security warrants is only involved in the issue of domestic interception warrants whereas foreign interception warrants, which are arguably closer to what GCSB’s authorised activities would involve, issued by a Minister alone.
\(^{25}\) It has been publicly confirmed that the Government intends to introduce a statute for GCSB.
\(^{26}\) This heading may confuse. Might “Qualified exemption to section 305ZFA offence for law enforcement agencies” be better?
for law enforcement agencies since the exemption might otherwise be construed to apply to other public sector agencies or even private bodies and persons.

3.5.3 I am satisfied with the exemption for executing an interception warrant. However, I have significant concerns about the exemption as it relates to execution of a search warrant or other legal authority.

**Search warrants**

3.5.4 In my view, it would be quite inappropriate to allow search warrants to be the legal basis for remotely accessing computers. Search warrants are not designed for regulating covert investigations or surveillance. Nonetheless, search warrants appropriately offer sufficient legal authority for accessing a person’s computer system from a computer on premises during entry onto premises pursuant to a warrant.

3.5.5 If I might interpolate at this point to say that it would be a valuable reform, from the perspective of individual privacy, to include in all laws governing the grant of search warrants a provision modelled upon that found in section 17 of the Serious Fraud Office Act 1990 (“notice the warrant has been executed, etc”). That section provides that any person executing a search warrant under that Act must, before leaving the place of search, place in a prominent position a written notice explaining that a search has been carried out and giving various other details including an inventory of documents removed during the search. This would seem to be a very valuable safeguard when a search has been carried out in the absence of the occupier of the premises.

3.5.6 A search warrant would be unsatisfactory as an authority for carrying out remote access to computers for a variety of reasons:

- there is no ability for the occupier to be present when his or her property is being searched;
- the questionable evidential value a covert search of a computer could have if not conducted under extremely carefully controlled circumstances to ensure reliability and admissibility of evidence. The search warrant process cannot begin to grapple with such issues;
- as an intrusive covert power, remote law enforcement hacking into a person’s computer should be, if allowed at all, very much a last resort. Search warrants, unlike interception warrants, do not require the intrusive technique to be used only as a last resort;
- interceptions warrants have strict requirements about the destruction of relevant and irrelevant records to ensure that the intrusion on privacy is proportionate to the objective. Search warrants do not establish a code as to such matters;
- a public reporting regime accompanies the grant of interception warrants but there is nothing similar for search warrants used in extraordinary circumstances;
- search warrants can be granted by persons without professional, legal and judicial experience and are unsuited to the imposition of carefully crafted conditions to protect the privacy of third parties.

3.5.7 It seems to me that law enforcement officials secretly snooping on peoples' computers, in circumstances where it will be a crime for others to do so, paints a highly distasteful picture. If that is ever to be justified it should be through a carefully prepared regime which establishes a new type of "computer access warrant" bringing with it careful authorisation processes and operations safeguards. Any covert police hacking should only be allowed in the most extraordinary circumstances and certainly not as a routine matter authorised by a simple search warrant.

3.5.8 I do not understand the police to have had any immediate desire or intention to undertake such hacking. Instead, I believe that the clause is simply a far too broadly drafted attempt to ensure that the existing practice of executing search warrants does not fall foul of the new computer access offence. I believe that all the police immediately need or want is a guarantee that when executing a search warrant on premises they are not hampered in attempting to search the contents of a computer found on the premises or in seizing the computer and to search it back at the police station. If indeed that is all they desire, it seems reasonable to me that they should have such an exemption from the law. However, the exemption should be written to encompass and legitimise the status quo and not to establish authority for new invasive practices at some future point. If such practices are to be authorised in the future, Parliament should revisit the matter.

Other legal authority

3.5.9 Moving to the final limb of the exemption: access gained under the exemption of "other legal authority". This suffers from most or all of the objections to access pursuant to search warrants but has the additional worrying feature that there may be no judicial authorisation or oversight at all depending on the nature of the "legal authority". The explanatory note to the bill gives little clue as to what is intended to be covered by the phrase "other lawful authority" but merely states that:

"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 activity."

3.5.10 In my view, a greater degree of certainty should be introduced into the provision if this third limb of the exemption is to remain. As with search warrants, the scope of the exemption should be sufficient to ensure that law enforcement is not hampered in its existing practices of search and inspection but not to authorise new and intrusive remote access practices. It would be less
objectionable I suggest if the “other lawful authority” phrase was replaced with a tighter exemption referring to:
• statutory authority expressly providing for access to computer systems; and
• access to computer systems found on premises searched or inspected pursuant to other lawful authority; or
• access to computer systems pursuant to other lawful authority carried out with the relevant person’s consent or in their presence.

3.5.11 In summary I recommend:
• that it be made explicit that the section 305ZFD exemption is available only to law enforcement agencies;
• that search warrant provisions be amended so that occupiers are given notice that a warrant has been executed, etc;
• that a search warrant constitute authority under the exemption only where the access is to a computer found on the premises being searched;
• that the phrase “other legal authority” be omitted or be modified to ensure that law enforcement hacking pursuant to other legal authority does not become a lawful practice.

3.6 Section 312Q - Commissioner of Police to give information to Parliament (clause 21M)

3.6.1 Public reporting about the nature and use of powers is an important feature of a scheme of safeguards when extraordinary and covert investigative powers are conferred on State agencies. To protect ongoing investigations such reporting can only be after the event. Nonetheless, it offers a picture to the general public and to interested persons, such as members of Parliament, about how the powers conferred are being utilised in practice.

3.6.2 Interception of private communications is supposed to be an exceptional law enforcement tool of last resort. Reported figures can provide some reassurance in that regard so that the public is comfortable that intrusive State surveillance is not becoming a routine technique. For example, it may reassure the public to know that the annual number of interception warrants issued to the NZSIS from 1980 to 1988 never exceeded five. If the number of warrants suddenly doubled or trebled one would expect questions to be asked. In the present context, it might be reassuring, or illuminating, to find out through reported figures whether the nature and scale of interception changes as a result of the new powers or exemptions.

Refer tabulation of reported details of NZSIS interception warrants in Report by the Privacy Commissioner to the Minister of Justice in relation to the New Zealand Security Intelligence Service Amendment Bill emphasising the Inadequacy of Public Reporting Obligations in relation to Interception Warrants, appendix 1, 9 February 1999.
3.6.3 Clause 21M amends the provision requiring reporting by the Police to Parliament about interception warrants and related matters by substituting “an interception device” wherever “a listening device” appears. A similar change is made to reporting obligations in the Misuse of Drugs Amendment Act 1978.\textsuperscript{28} In my opinion, it would be desirable to amend the reporting obligations in two ways:

- to require reporting of meaningful figures which reflect the new expanded scope of interception warrants into non-oral communications;
- to require the reporting of qualitative information which explains the quantitative material.

3.6.4 In the past, interception warrants have been used to authorise the interception only of oral communications. In the future, it is likely that faxes and emails and other forms of non-oral communication will also be intercepted. For the reported figures to meaningfully inform Parliament and the public about the effect of the expansion of authorised interceptions and the manner in which powers granted are indeed being used, it is desirable for the reported figures to distinguish between existing interceptions and matters currently reported (that is oral communications intercepted by telephone taps and the placing of bugs) and the new range of non-oral communications. At the very least, reports should distinguish between the interception of oral and non-oral communications. It is already a requirement on the NZSIS to report the “method of interception” and so a picture should emerge from its reports as to any increasing interception trends affecting email and the like.\textsuperscript{29}

3.6.5 Currently, the Police Commissioner merely lists the information that is required to be reported in a relatively uninformative fashion. The NZ Police annual report merely lists the section under which applications are made followed with a series of numbers of applications etc for the year in question. No assistance is given to the reader. For example, there are details given under the heading “applications made under section 14” of the Misuse of Drugs Amendment Act 1978. This is followed by a list of figures about “applications made under section 15A”. No explanation is given as to what sections 14 and 15A refer to.\textsuperscript{30} Nor are figures for any previous year given to enable readers to identify trends. To make much sense of the reported figures a reader would have to obtain:

- the Police Commissioner’s current annual report;
- the Commissioner’s previous annual reports;
- a copy of the relevant provisions in the Crimes Act;
- a copy of the relevant provisions in the Misuse of Drugs Act 1978.

Even then, a person studying the figures is without the benefit of the Police Commissioner’s opinion about important trends or significant figures reported in the current year.

\textsuperscript{28} Refer Schedule 3 to the Supplementary Order Paper.

\textsuperscript{29} NZSIS Act, section 4K.

\textsuperscript{30} Section 14 of the Misuse of Drugs Amendment Act concerns interception warrants for “drug dealing offences” whereas section 15A concerns “prescribed cannabis offences” which involve “dealing in cannabis on a substantial scale”.

16
3.6.6 As I have observed previously, it should not need an amendment to the Act for the Police to report more meaningful information for the benefit of Parliament and public. However, as it seems clear from the reports of successive Police Commissioners that the Police will only report that which is explicitly required, I recommend that the Act impose obligations to explain statistics and trends. A corresponding change would also need to be made to section 29 of the Misuse of Drugs Amendment Act 1978.

4. UNFINISHED BUSINESS

4.1 The scheme for authorising and overseeing law enforcement interception of private communication under the Crimes Act follows the model established in the Misuse of Drugs Amendment Act 1978. That Act was introduced and passed in the first term of the government of Rt Hon Sir Robert Muldoon in the lead up to the 1978 general election. The Opposition was given a copy of the bill only 10 minutes before its introduction on 5 September 1978. Three oral submissions were permitted by the House to be taken and a further 15 written submissions received in the short time allowed. The bill was reported back from the Select Committee three weeks later on 26 September and signed into law on 16 October. While aspects of the 1978 scheme are perfectly satisfactory from a privacy perspective, particularly the involvement of a judge in granting warrants, the scheme does not contain the range of safeguards for the protection of civil rights and privacy found in modern legislation overseas.

4.2 It is unsurprising that a 1978 law, enacted hurriedly in the politically charged atmosphere of a general election, falls short of international best practice in terms of individual rights and liberties 20 years later. The 1978 law model has since been duplicated into three further powers of interception. While the scope of interception has significantly expanded, occasionally some of even the limited safeguards adopted in 1978 have been whittled away.

4.3 In my view, there is a case for a systematic re-examination of aspects of our interception law in order to enhance desirable transparency, accountability, oversight, control and respect for privacy (rather than as a platform for law enforcement to continually seek to expand powers further and chip away at existing constraints). If there were to be such a review, it could also look at the related statutory schemes concerning tracking devices, telephone analysers, opening of postal articles, powers of entry onto private premises and into

31 Report by the Privacy Commissioner to the Minister of Justice on Parts V and VIII of the Harassment and Criminal Associations Bill, 28 April 1997, paras 5.9-5.10 and related paragraphs.
32 The original provisions in the Misuse of Drugs Amendment Act 1978, section 14, was joined by section 15A in 1998, while the Crimes Act 1961, sections 312B and 312CA, were added in 1987 and 1998 respectively.
33 For example, the prohibition on making oral applications for emergency permits for telephonic interception was repealed in 1997.
34 Misuse of Drugs Act 1975, section 33.
35 See Telecommunications Act, section s10A - 10S.
computer systems and the licensing of private investigators.\textsuperscript{37} A review could also look at largely unregulated areas of covert video surveillance and the use of human intelligence sources.\textsuperscript{38}

4.4 Notwithstanding the absence of any systematic review, I have attempted to raise concrete suggestions for enhancement of privacy and citizens' rights as opportunities have arisen with \textit{ad hoc} amendments to the laws governing interception of private communications and law enforcement and intelligence agencies. I have reported to Ministers of Justice since 1993 as follows:

\textbf{Interception of private communications}
- Harassment and Criminal Associations Bill (April 1997)

\textbf{Intelligence agencies}
- Immigration Amendment Bill 1998 (November 1998)
- New Zealand Security Intelligence Service Amendment Bill (February 1999)
- New Zealand Security Intelligence Service Amendment Bill (No 2) (April 1999)

\textbf{Related reports}
- Postal Services Bill (June 1997)
- Telephone Analysers and Call Data Warrants (September 1997)
- Radiocommunications Amendment Bill (January 1998)
- Penal Institutions Amendment Bill (No 2): Monitoring Inmate Telephone Calls (August 1999)
- Necessary and Desirable: Privacy Act 1993 Review (December 1998)
- Transport Accident Investigation Amendment Bill (March 1999).

4.5 In each of these reports I have focused on the bills under consideration and made specific recommendations for amendment, a number of which have been adopted. However, sometimes these bills have highlighted issues which have not been able to be satisfactorily addressed since they would involve further policy work and require amendment to laws other than the bills under consideration. Accordingly, I take the opportunity to once again raise some of these suggestions.

\textbf{Major suggestions for enhancing interception safeguards}

4.6 My principal previous report on the subject was in relation to the Harassment and Criminal Association Bill. I expressed the view in that report that the time is right for the introduction of new safeguards into the processes for interception of private communications and noted that:

\textsuperscript{37} Private Investigators and Security Guards Act 1974.
\textsuperscript{38} The phrase "human intelligence sources" is taken from the recent Regulation of Investigatory Powers Act 2000 (UK).
• while our law remained based on a 1978 model, Australia, Canada and the UK, have all introduced enhanced safeguards or oversight mechanisms in recent years;
• technological changes have meant that the nature of electronic surveillance has changed, and is changing, and enhancement and review of safeguards may provide better oversight for proposals to vary or expand police power;
• beyond the very limited (although important) involvement of the judiciary there is no independent scrutiny or audit of what actually occurs after the warrant is issued and it is desirable that this gap be filled if the public are to have assurance that State surveillance is always conducted according to law.

In my report, I explained at length my reasoning for proposing three new safeguards and cited a number of overseas precedents. While such reforms could be described as major, each is based on safeguards already existing in other jurisdictions.

4.7 It appears that there are two major safeguards in overseas laws having no equivalent in New Zealand. These are:
• notification to individuals after the event of the fact that their private communications have been intercepted (which might be called “the notification model”);
• requiring full documentation of every authorised interception and conferring audit and oversight functions on a body independent from the agency which undertakes the interception (“the audit model”).

4.8 Notification is the requirement in Germany, the United States and elsewhere. Audit operates in Australia. In my earlier report I noted the conclusions of the Hong Kong Law Reform Commission, which had recently studied the matter in detail, that audit had clear advantages over the notification model. In making my earlier recommendations I favoured the audit model while keeping the notification requirement for exceptional cases. Notification is a powerful privacy and civil rights protection which should not lightly be dismissed from consideration. (It might also be considered a necessary technical requirement for both the individual in question and the owner of a private computer or communications system.) I also suggested a right to compensation for unlawful interception — whether by the Police or anyone else. Compensation, my third proposal, can work with either model or with the existing law.

4.9 The proposed safeguards are:
(a) to create an interception register and have this audited by a suitable independent body such as the Police Complaints Authority;
(b) to grant that independent body a power to require the Police, in exceptional cases, to notify individuals whose communications have been intercepted of the fact, at a suitable point after the interception or investigation is completed;
(c) to establish a right to compensation for unlawful interception.

Other recommendations: law enforcement

4.10 I have made a number of recommendations relating to the provisions for authorised interception of private communications by law enforcement agencies. I mention several of them below as illustrative of “unfinished business” which could appropriately be taken up if an appropriate opportunity arises. As I have taken an illustrative rather than comprehensive approach, the following does not encompass all previous recommendations nor all those that I might make if there were to be a thorough review. In this context, I do not offer any justification for the suggestions but full reasoning can be found in the text of the relevant report.

4.11 Suggestions for change to present interception law include (in no particular order):

- Oral applications for emergency permits should be able to made only by a Police officer of a certain specified rank or with the approval of such an officer.  

- Further information concerning the nature of interception should be annually reported to Parliament including:
  
  (a) methods of interception - such as “telecommunications”, “microphone”, “video” and “other” to use the Canadian reporting breakdown;  
  
  (b) general description of the classes of places specified in warrants - in Canada the categories utilised are “residence (permanent)”, “residence (temporary)”, “commercial premises”, “vehicles” and “other”;
  
  (c) number of persons identified through interception and average number of persons identified per warrant - interception of private communications does not simply involve an intrusion into the privacy of targeted individuals but affects all who come into contact with them, their telephone or their premises - for instance, 1994 figures from Canada showed that 26.7 people on average were identified as listened to for each authorised interception while 1992 data from the USA suggested that 117 people were monitored per installed intercept and the average number of conversations intercepted was 1861;  
  
  (d) categories of offenses.  

- A judicial warrant process should be established in relation to the use of covert video surveillance in the investigation of offences.

- The powers relating to the opening and inspection of postal articles for the purposes of law enforcement should be reformed so that:
  
  (a) postal operators are obliged to keep a record of the exercise of powers of detention, opening and inspection with these records subjected both to public reporting obligations in aggregate form and inspection and audit by appropriate authorities;

---

40 Report by the Privacy Commissioner to the Minister of Justice on Parts V and VIII of the Harassment and Criminal Associations Bill, Interception of Private Communications, 28 April 1997, para 3.3.
41 Ibid, para 3.4.8(a).
42 Ibid, para 3.4.9(b).
43 Ibid, para 3.4.9(c).
44 Ibid, para 3.4.9(d).
45 Privacy Commissioner, Necessary and Desirable Privacy Act 1993 Review, recommendation 22, para 2.6.5.
(b) where letters are opened then resealed and delivered, appropriate notice should be given to both the addressee and the sender;
(c) re-consideration should be given to whether and how private postal operators should exercise powers of opening mail.\textsuperscript{46}

Other recommendations: intelligence and security agencies

I have already in this report recommended that GCSB should be placed on a statutory footing. A few suggestions for change to present law governing intelligence and security agencies are offered (in no particular order):

- provisions governing the NZSIS function of vetting civil servants should be placed on an explicit statutory footing (with a greater degree of openness than is appropriate for other covert aspects of that agency’s activities);\textsuperscript{47}
- the partial exemption for intelligence agencies from the information privacy principles should be narrowed so that the NZSIS and GCSB additionally become subject to principles 1, 5, 8 and 9;\textsuperscript{48}
- consideration should be given to having foreign intelligence warrants issued by the responsible Minister and the Commissioner of Security Warrants jointly as is the case with domestic interception warrants;\textsuperscript{49}
- the maximum term of an interception warrant for the NZSIS should be reduced from 12 to 6 months.\textsuperscript{50}

5. SUMMARY OF CONCLUSIONS AND RECOMMENDATIONS

5.1 I support the enactment of criminal laws to better protect privacy by:
- extending the prohibition against intercepting private communications to include non-oral communications;
- prohibiting unauthorised access to computer systems.

5.2 I accept that there is a case to create appropriate exemptions to these new laws. It is essential that covert interception and computer access be limited to the level absolutely necessary to enable the relevant agencies to perform their proper functions. It must be subject to careful authorisation processes and operational controls, and be proportionate to the intrusion on privacy. My principal concerns about the bill relate to the exemptions and, in particular, to the lack of controls on ISPs and GCSB in relation to the expanded interception offence, and to the law enforcement and GCSB exemption in relation to the computer access

\textsuperscript{46} Report by the Privacy Commissioner to the Minister of Justice on the Postal Services Bill, June 1997, recommendations 5.2, 5.4, 5.5, 5.6-5.8.
\textsuperscript{47} Report of the Privacy Commissioner to the Minister of Justice on the Intelligence and Security Agencies Bill, February 1996, para 5.2.
\textsuperscript{49} Report by the Privacy Commissioner to the Minister of Justice in relation to the New Zealand Security Intelligence Service Amendment Bill (No 2), April 1999, para 6.4(b).
\textsuperscript{50} Ibid, para 6.4(c).
offence. In each case, I suggest law changes which would more appropriately protect privacy while allowing such exemptions.

5.3 I make the following recommendations for amendment to the provisions in Supplementary Order Paper No 85:

Section 216A(1)

1. The definition of “interception device” should be amended by omitting the provision for exempting devices from the provisions of Part Ixa of the Crimes Act by Order in Council. However, if the exemption power is to be retained:
   (a) the purpose for granting such exemptions should be made explicit and limited; and
   (b) such Orders be subject to a sunset clause at the expiry of which they must have been confirmed by Parliament or expire.
   (paras 3.1.1 – 3.1.7)

Section 216B(5)

2. As a prerequisite to granting an exemption for GCSB from the prohibition on use of listening devices, the Bureau should:
   (a) be placed on a statutory footing; and
   (b) be subject to a statutory warrant process for the undertaking of any intrusive activity particularly where that activity would, if performed by any other person, constitute a breach of the law.
   (paras 3.2.2 – 3.2.5)

3. The GCSB exemption in section 216B(5) should either:
   (a) state the place from which interception may be carried out; or
   (b) state that interception may be carried out only from a place described in an Order in Council.
   (paras 3.2.6 – 3.2.8)

Section 216B(6)

4. Evidence should be obtained by, or placed before, the Select Committee studying the bill to establish whether there really is a need for Internet Service Providers to have access to the content of private communications for the purpose of maintaining communication services. If such access is not essential the exemption should not be granted.
   (paras 3.2.9 – 3.2.11)

5. Assuming an exemption for ISPs to be necessary, section 216B(6) should be amended to emphasise that accessing the content of messages should only occur where there is no practical alternative. A
suitable new paragraph (c) could state “The interception is essential for that purpose.”
(paras 3.2.11 – 3.2.13)

6. In all cases where there is an exemption from the prohibition against intercepting private communications for particular purposes, there ought to be an accompanying statutory prohibition on retaining, using and disclosing the information for other purposes except where required by law. Part IXA of the Crimes Act ought to provide that:
(a) any information obtained by the persons benefiting from the exemptions in sections 216B(2)(b)(ii) and 216B(6) must only be used for the purpose of maintaining the telecommunication, Internet or other communication service;
(b) such information must not be disclosed to anyone, other than the individuals concerned, except where required by law; and
(c) such information must be promptly destroyed when no longer needed for the purpose of maintaining the telecommunication, Internet or other communication service;
(d) breach of (a), (b) and (c) to constitute an offence.
(paras 3.2.11 – 3.2.12)

Section 305ZFA

7. Consideration should be given to whether section 305ZFA(2) can usefully be clarified.
(paras 3.3.3 – 3.3.6)

Section 305ZFC

8. As a prerequisite to granting an exemption for GCSB from the prohibition on unauthorised access to computer systems, the Bureau should:
(a) be placed on a statutory footing; and
(b) be subject to a statutory warrant process for the undertaking of any such areas.
(paras 3.4.3 - 3.4.6)

Section 305ZFD

9. The section 305ZFD exemption should explicitly be limited only to law enforcement agencies.
(paras 3.5.2, 3.5.11)

10. Search warrants should not provide legal authority for remotely accessing computers in a type of “Police hacking”. Instead, section 305ZFD should be amended so that a search warrant merely provides authority to search the contents of a computer found on premises being searched pursuant to that warrant.
(paras 3.5.4 - 3.5.8, 3.5.11)
11. Reference to "other lawful authority", which provides an exemption in section 305ZFD to the prohibition on unauthorised accessing of computers should be replaced with a tighter exemption referring to:
(a) statutory authority *expressly* providing for access to computer systems;
(b) access to computers found on premises searched or inspected pursuant to other lawful authority;
(c) accessing computer systems pursuant to other lawful authority carried with the relevant person’s consent or in their presence.

(paras 3.5.9 - 3.5.11)

Section 312Q (and Misuse of Drugs Amendment Bill Act 1978, section 29)

12. The provisions concerning annual reporting requirements of the Police Commissioner in relation to interception warrants should be amended to:
(a) distinguish between oral and non-oral interceptions;
(b) require an explanation as to figures presented including trends and significant or unexpected results.

(paras 3.6.1 - 3.6.6)

Further recommendations

13. Provisions in statutes providing for the issue and executions of search warrants should be amended so that occupiers are given notice that a warrant has been executed if the search is carried out in their absence.

(paras 3.5.3, 3.5.11)

14. Consideration should be given to revising and enhancing the statutory and operational safeguards governing statutory powers of covert investigation. If not done in a comprehensive review, I urge consideration of the various *ad hoc* recommendations I have made in the last few years summarised in this report.

(paras 4.1 - 4.11)

B H Slane
Privacy Commissioner
13 December 2000