Telecommunications (Interception) Amendment Act 2006

No. 40, 2006

An Act to amend the *Telecommunications (Interception) Act 1979*, and for related purposes

Note: An electronic version of this Act is available in ComLaw (http://www.comlaw.gov.au/)

Contents

Telecommunications (Interception) Amendment Act 2006

No. 40, 2006

An Act to amend the *Telecommunications (Interception) Act 1979*, and for related purposes

[*Assented to 3 May 2006*]

The Parliament of Australia enacts:

1 Short title

This Act may be cited as the *Telecommunications (Interception) Amendment Act 2006*.

2 Commencement

(1) Each provision of this Act specified in column 1 of the table commences, or is taken to have commenced, in accordance with column 2 of the table. Any other statement in column 2 has effect according to its terms.

Commencement information

Column 1 Provision(s)	Column 2 Commencement	Column 3 Date/Details
1. Sections 1 to 3 and anything in this Act not elsewhere covered by this table	The day on which this Act receives the Royal Assent.	3 May 2006
2. Schedules 1 to 3	A single day to be fixed by Proclamation. However, if any of the provision(s) do not commence within the period of 6 months beginning on the day on which this Act receives the Royal Assent, they commence on the first day after the end of that period.	13 June 2006 (*see* F2006L01623)
3. Schedule 4	1 July 2006.	1 July 2006
4. Schedule 5	A single day to be fixed by Proclamation. However, if any of the provision(s) do not commence within the period of 6 months beginning on the day on which this Act receives the Royal Assent, they commence on the first day after the end of that period.	3 November 2006
5. Schedule 6, item 1	Immediately after the commencement of item 10 of Schedule 1 to the *Telecommunications (Interception) Amendment (Stored Communications and Other Measures) Act 2005*.	1 October 2006
6. Schedule 6, item 2	The day on which this Act receives the Royal Assent.	3 May 2006
7. Schedule 6, item 3	Immediately after the commencement of item 10 of Schedule 1 to the *Telecommunications (Interception) Amendment (Stored Communications and Other Measures) Act 2005*.	1 October 2006

Commencement information		
Column 1	**Column 2**	**Column 3**
Provision(s)	**Commencement**	**Date/Details**
8. Schedule 6, items 4 to 7	The day on which this Act receives the Royal Assent.	3 May 2006
9. Schedule 6, item 8	Immediately after the commencement of section 17 of the *Telecommunications (Interception) Amendment Act 1993*.	1 February 1994
10. Schedule 6, items 9 and 10	The day on which this Act receives the Royal Assent.	3 May 2006

Note: This table relates only to the provisions of this Act as originally passed by the Parliament and assented to. It will not be expanded to deal with provisions inserted in this Act after assent.

(2) Column 3 of the table contains additional information that is not part of this Act. Information in this column may be added to or edited in any published version of this Act.

3 Schedule(s)

Each Act that is specified in a Schedule to this Act is amended or repealed as set out in the applicable items in the Schedule concerned, and any other item in a Schedule to this Act has effect according to its terms.

Schedule 1—Stored communications

Part 1—Principal amendments

Telecommunications (Interception) Act 1979

1 Subsection 5(1)

Insert:

stored communication means a communication that:

(a) is not passing over a telecommunications system; and

(b) is held on equipment that is operated by, and is in the possession of, a carrier; and

(c) cannot be accessed on that equipment, by a person who is not a party to the communication, without the assistance of an employee of the carrier.

2 After section 5D

Insert:

5E Serious contraventions

(1) For the purposes of this Act, a ***serious contravention*** is a contravention of a law of the Commonwealth, a State or a Territory that:

(a) is a serious offence; or

(b) is an offence punishable:

(i) by imprisonment for a period, or a maximum period, of at least 3 years; or

(ii) if the offence is committed by an individual—by a fine, or a maximum fine, of at least 180 penalty units; or

(iii) if the offence cannot be committed by an individual—by a fine, or a maximum fine, of at least 900 penalty units; or

(c) could, if established, render the person committing the contravention liable:

(i) if the contravention were committed by an individual—to pay a pecuniary penalty of 180 penalty units or more,

or to pay an amount that is the monetary equivalent of 180 penalty units or more; or

(ii) if the contravention cannot be committed by an individual—to pay a pecuniary penalty of 900 penalty units or more, or to pay an amount that is the monetary equivalent of 900 penalty units or more.

(2) Except so far as the contrary intention appears, a contravention, or a contravention of a particular kind, is taken, for the purposes of this Act, to be a contravention, or to be a contravention of that kind, as the case may be, that:

(a) has been committed or is being committed; or

(b) is suspected on reasonable grounds of having been committed, of being committed or of being likely to be committed.

(3) To avoid doubt, a reference in this section to a number of penalty units in relation to a contravention of a law of a State or a Territory includes a reference to an amount of a fine or pecuniary penalty that is equivalent, under section 4AA of the *Crimes Act 1914*, to that number of penalty units.

5F When a communication is passing over a telecommunications system

(1) For the purposes of this Act, a communication:

(a) is taken to start passing over a telecommunications system when it is sent or transmitted by the person sending the communication; and

(b) is taken to continue to pass over the system until it becomes accessible to the intended recipient of the communication.

(2) However, if a communication is sent from an address on a computer network operated by or on behalf of the Australian Federal Police, it is taken not to start passing over a telecommunications system, for the purposes of this Act, until it is no longer under the control of any of the following:

(a) any AFP employee responsible for operating, protecting and maintaining the network;

(b) any AFP employee responsible for enforcement of the professional standards of the Australian Federal Police.

(3) Subsection (2) ceases to have effect at the end of the period of 2 years starting at the commencement of this section.

5G The intended recipient of a communication

(1) For the purposes of this Act, the ***intended recipient*** of a communication is:

(a) if the communication is addressed to an individual (either in the individual's own capacity or in the capacity of an employee or agent of another person)—the individual; or

(b) if the communication is addressed to a person who is not an individual—the person; or

(c) if the communication is not addressed to a person—the person who has, or whose employee or agent has, control over the telecommunications service to which the communication is sent.

(2) In addition to the person who is the intended recipient of a communication under subsection (1), if a communication is addressed to a person at an address on a computer network operated by or on behalf of the Australian Federal Police, each of the following is also an ***intended recipient*** of the communication for the purposes of this Act:

(a) any AFP employee responsible for operating, protecting and maintaining the network;

(b) any AFP employee responsible for enforcement of the professional standards of the Australian Federal Police.

(3) Subsection (2) ceases to have effect at the end of the period of 2 years starting at the commencement of this section.

(4) If subsection (2) applies to a communication, a reference in this Act (other than in this section) to the intended recipient of the communication is taken to be a reference to an intended recipient of the communication.

5H When a communication is accessible to the intended recipient

(1) For the purposes of this Act, a communication is ***accessible*** to its intended recipient if it:

(a) has been received by the telecommunications service provided to the intended recipient; or

(b) is under the control of the intended recipient; or

(c) has been delivered to the telecommunications service provided to the intended recipient.

(2) Subsection (1) does not limit the circumstances in which a communication may be taken to be accessible to its intended recipient for the purposes of this Act.

3 After section 6

Insert:

6AA Accessing a stored communication

For the purposes of this Act, ***accessing*** a stored communication consists of listening to, reading or recording such a communication, by means of equipment operated by a carrier, without the knowledge of the intended recipient of the communication.

4 After section 6DA

Insert:

6DB Issuing authorities

(1) The Minister may, by writing, appoint as an issuing authority:

(a) a person who is:

(i) a judge of a court created by the Parliament; or

(ii) a Federal Magistrate; or

(iii) a magistrate;

and in relation to whom a consent under subsection (2) is in force; or

(b) a person who:

(i) holds an appointment to the Administrative Appeals Tribunal as Deputy President, full-time senior member, part-time senior member or member; and

(ii) is enrolled as a legal practitioner of a federal court or of the Supreme Court of a State or a Territory; and

(iii) has been enrolled for at least 5 years.

(2) A person who is:

(a) a judge of a court created by the Parliament; or
(b) a Federal Magistrate; or
(c) a magistrate;

may, by writing, consent to be appointed by the Minister under subsection (1).

(3) A person's appointment ceases to have effect if:
(a) the person ceases to be a person whom the Minister could appoint under this section; or
(b) the Minister, by writing, revokes the appointment.

(4) An issuing authority has, in relation to the performance or exercise of a function or power conferred on an issuing authority by this Act, the same protection and immunity as a Justice of the High Court has in relation to proceedings in the High Court.

5 After section 6EA

Insert:

6EB Stored communications warrant information

A reference in this Act to ***stored communications warrant information*** is a reference to:

(a) information about any of the following:
(i) an application for a stored communications warrant;
(ii) the issue of a stored communications warrant;
(iii) the existence or non-existence of a stored communications warrant;
(iv) the expiry of a stored communications warrant; or
(b) any other information that is likely to enable the identification of:
(i) the telecommunications service to which a stored communications warrant relates; or
(ii) a person specified in a stored communications warrant as a person using or likely to use the telecommunications service to which the warrant relates.

6 After subsection 9(1)

Insert:

(1A) The reference in paragraph (1)(b) to the interception of communications made to or from a telecommunications service includes a reference to the accessing of the communications as stored communications after they have ceased to pass over a telecommunications system.

7 After subsection 9A(1)

Insert:

(1A) The reference in paragraph (1)(b) to the interception of communications made to or from a telecommunications service includes a reference to the accessing of the communications as stored communications after they have ceased to pass over a telecommunications system.

8 After subsection 10(1)

Insert:

(1A) The reference in subparagraph (1)(d)(ii) to the interception not commencing includes a reference to the communications, that were to be intercepted, not being accessed as stored communications after they have ceased to pass over a telecommunications system.

9 After Part XA

Insert:

Chapter 3—Access to stored communications

Part 3-1—Prohibition on access to stored communications

108 Stored communications not to be accessed

(1) A person commits an offence if:

(a) the person:

(i) accesses a stored communication; or

(ii) authorises, suffers or permits another person to access a stored communication; or

(iii) does any act or thing that will enable the person or another person to access a stored communication; and

(b) the person does so with the knowledge of neither of the following:

(i) the intended recipient of the stored communication;

(ii) the person who sent the stored communication.

Penalty: Imprisonment for 2 years or 120 penalty units, or both.

Note: This section does not prohibit accessing of communications, that are no longer passing over a telecommunications system, from the intended recipient or from a telecommunications device in the possession of the intended recipient.

(1A) Without limiting paragraph (1)(b), a person is taken for the purposes of that paragraph to have knowledge of an act referred to in paragraph (1)(a) if written notice of an intention to do the act is given to the person.

Note: For giving notice, see section 28A of the *Acts Interpretation Act 1901*.

(2) Subsection (1) does not apply to or in relation to:

(a) accessing a stored communication under a stored communications warrant; or

(b) accessing a stored communication under an interception warrant; or

(c) accessing a stored communication under a computer access warrant issued under section 25A of the *Australian Security Intelligence Organisation Act 1979*; or

(d) an act or thing done by an employee of a carrier in the course of his or her duties for or in connection with:

(i) the installation of any line, or the installation of any equipment, used or intended for use in connection with a telecommunications service; or

(ii) the operation or maintenance of a telecommunications system; or

(iii) the identifying or tracing of any person who has contravened, or is suspected of having contravened or being likely to contravene, a provision of Part 10.6 of the *Criminal Code*;

if it is reasonably necessary for the employee to do that act or thing in order to perform those duties effectively; or

(e) accessing a stored communication by another person lawfully engaged in duties relating to the installation, connection or maintenance of equipment or a line, if it is reasonably necessary for the person to access the communication in order to perform those duties effectively; or

(f) accessing a stored communication by a person lawfully engaged in duties relating to the installation, connection or maintenance of equipment used, or to be used, for accessing stored communications under:

(i) stored communications warrants; or

(ii) interception warrants; or

(iii) computer access warrants issued under section 25A of the *Australian Security Intelligence Organisation Act 1979*; or

(g) accessing a stored communication if the access results from, or is incidental to, action taken by an officer of the Organisation, in the lawful performance of his or her duties, for the purpose of:

(i) discovering whether a listening device is being used at, or in relation to, a particular place; or

(ii) determining the location of a listening device; or

(h) accessing a stored communication by an officer or staff member of the Australian Communications and Media Authority engaged in duties relating to enforcement of the *Spam Act 2003*.

Note: A defendant bears an evidential burden in relation to the matter in subsection (2) (see subsection 13.3(3) of the *Criminal Code*).

(3) For the purposes of paragraph (2)(b), access to a stored communication is taken to be under an interception warrant if, and only if, the warrant would have authorised interception of the communication if it were still passing over a telecommunications system.

(4) In determining, for the purposes of paragraphs (2)(d) and (e), whether an act or thing done by a person was reasonably necessary in order for the person to perform his or her duties effectively, a court is to have regard to such matters (if any) as are specified in, or ascertained in accordance with, the regulations.

Note: The civil remedy provisions in Part 3-7 may apply to a contravention of this section.

Part 3-2—Access by the Organisation to stored communications

109 Access to stored communications under Part 2-2 warrants

In addition to authorising interception of communications, a Part 2-2 warrant also authorises a person to access a stored communication if:

(a) the warrant would have authorised interception of the communication if it were still passing over a telecommunications system; and

(b) the person is approved under section 12 in respect of the warrant.

Part 3-3—Access by enforcement agencies to stored communications

Division 1—Applications for warrants

110 Enforcement agencies may apply for stored communications warrants

(1) An enforcement agency may apply to an issuing authority for a stored communications warrant in respect of a person.

(2) The application must be made on the agency's behalf by:

(a) if the agency is referred to in subsection 39(2)—a person referred to in that subsection in relation to that agency; or

(b) otherwise:

(i) the chief officer of the agency; or

(ii) an officer of the agency (by whatever name called) who holds, or is acting in, an office or position in the agency nominated under subsection (3).

(3) The chief officer of the agency may, in writing, nominate for the purposes of subparagraph (2)(b)(ii) an office or position in the agency that is involved in the management of the agency.

(4) A nomination under subsection (3) is not a legislative instrument.

111 Form of applications

(1) The application must be in writing.

(2) However, a person making the application on the agency's behalf may make the application by telephone if the person:
  (a) is the chief officer of the agency or a person in relation to whom an authorisation by the chief officer is in force under subsection (3); and
  (b) thinks it necessary, because of urgent circumstances, to make the application by telephone.

(3) The chief officer of an enforcement agency may, in writing, authorise persons (including classes of persons) for the purposes of subsection (2). However, each person must be entitled under section 110 to make applications on the agency's behalf.

112 Contents of written applications

The application must, if it is in writing, set out:
  (a) the name of the agency; and
  (b) the name of the person making the application on the agency's behalf.

113 Affidavits to accompany written applications

(1) The application must, if it is in writing, be accompanied by an affidavit complying with this section.

(2) The affidavit must set out the facts and other grounds on which the application is based.

(3) Despite subsection (1), a written application may be accompanied by 2 or more affidavits that together set out each matter that, but for this subsection, this section would have required an affidavit accompanying the application to set out.

114 Information to be given on telephone applications

The information given to an issuing authority in connection with a telephone application to the issuing authority:
  (a) must include particulars of the urgent circumstances because of which the person making the application on the agency's

behalf thinks it necessary to make the application by telephone; and

(b) must include each matter that, if the application had been made in writing, section 112 or 113 would have required the application, or an affidavit accompanying it, to set out; and

(c) must be given orally or in writing, as the issuing authority directs.

115 Giving further information to Judge

(1) An issuing authority may require further information to be given in connection with an application to the issuing authority for a warrant.

(2) The further information:

(a) must be given on oath if the application was made in writing; and

(b) must be given orally or otherwise, as the issuing authority directs.

Division 2—Issuing of warrants

116 Issuing of stored communications warrants

(1) An issuing authority to whom an enforcement agency has applied for a stored communications warrant in respect of a person may, in his or her discretion, issue such a warrant if satisfied, on the basis of the information given to him or her under this Part in connection with the application, that:

(a) Division 1 has been complied with in relation to the application; and

(b) in the case of a telephone application—because of urgent circumstances, it was necessary to make the application by telephone; and

(c) there are reasonable grounds for suspecting that a particular carrier holds stored communications:

(i) that the person has made; or

(ii) that another person has made and for which the person is the intended recipient; and

(d) information that would be likely to be obtained by accessing those stored communications under a stored communications warrant would be likely to assist in connection with the investigation by the agency of a serious contravention in which the person is involved; and

(e) having regard to the matters referred to in subsection (2), and to no other matters, the issuing authority should issue a warrant authorising access to such stored communications.

(2) The matters to which the issuing authority must have regard are:

(a) how much the privacy of any person or persons would be likely to be interfered with by accessing those stored communications under a stored communications warrant; and

(b) the gravity of the conduct constituting the serious contravention; and

(c) how much the information referred to in paragraph (1)(d) would be likely to assist in connection with the investigation; and

(d) to what extent methods of investigating the serious contravention that do not involve the use of a stored communications warrant in relation to the person have been used by, or are available to, the agency; and

(e) how much the use of such methods would be likely to assist in connection with the investigation by the agency of the serious contravention; and

(f) how much the use of such methods would be likely to prejudice the investigation by the agency of the serious contravention, whether because of delay or for any other reason.

(3) The warrant may be issued in relation to the investigation of more than one serious contravention.

117 What stored communications warrants authorise

A stored communications warrant authorises persons approved under subsection 127(2) in respect of the warrant to access, subject to any conditions or restrictions that are specified in the warrant, a stored communication:

(a) that was made by the person in respect of whom the warrant was issued; or

(b) that another person has made and for which the intended recipient is the person in respect of whom the warrant was issued;

and that becomes, or became, a stored communication before the warrant is first executed in relation to the carrier that holds the communication.

118 Form and content of stored communications warrants

(1) A stored communications warrant:

(a) must be in accordance with the prescribed form; and

(b) must be signed by the issuing authority who issues it.

(2) A stored communications warrant may specify conditions or restrictions relating to accessing stored communications under the warrant.

(3) A stored communications warrant must set out short particulars of each serious contravention in relation to which the issuing authority issuing the warrant was satisfied, on the application for the warrant, as mentioned in paragraph 116(1)(d).

119 Duration of stored communications warrants

(1) A stored communications warrant remains in force:

(a) until it is first executed; or

(b) until the end of the period of 5 days after the day on which it was issued;

whichever occurs sooner.

(2) However, if the warrant relates to more than one telecommunications service and those services are not all operated by the same carrier, the warrant remains in force, to the extent that it relates to a telecommunications service operated by a particular carrier:

(a) until it is first executed in relation to a telecommunications service operated by that particular carrier; or

(b) until the end of the period of 5 days after the day on which it was issued;

whichever occurs sooner.

(3) An issuing authority must not vary a stored communications warrant by extending the period for which it is to be in force.

(4) This section does not prevent the issue of a further warrant in respect of the person in respect of whom the warrant was issued.

(5) However, if the further warrant relates to the same telecommunications service as the previous warrant, it must not be issued within 3 days after the day on which the previous warrant was executed or (if subsection (2) applies) was last executed.

Division 3—How warrants etc. are dealt with

120 Stored communications warrants issued on telephone applications

(1) An issuing authority who issues a stored communications warrant on a telephone application:

(a) must, as soon as practicable after completing and signing the warrant:

(i) inform the person who made the application, on behalf of the enforcement agency concerned, of the terms of the warrant, the day on which it was signed and the time at which it was signed; and

(ii) give the warrant to that person; and

(b) must keep a copy of the warrant.

(2) A person who makes a telephone application on an enforcement agency's behalf must, within one day after the day on which a warrant is issued on the application:

(a) cause each person who gave information to the issuing authority in connection with the application to swear an affidavit setting out the information so given by the person; and

(b) give to the issuing authority:

(i) the affidavit or affidavits; and

(ii) unless the applicant is the chief officer of the enforcement agency—a copy of an authorisation by the chief officer under subsection 111(3) that was in force in relation to the applicant when the application was made.

(3) An issuing authority may, by writing signed by him or her, revoke a warrant that he or she issued on a telephone application if satisfied that subsection (2) has not been complied with in relation to the warrant. If he or she does so, he or she must:

(a) forthwith inform the person who made the application on the enforcement agency's behalf, or the chief officer of the enforcement agency, of the revocation; and

(b) give the instrument of revocation to that person, or to the chief officer, as soon as practicable.

(4) The chief officer of that agency must, if another enforcement agency is exercising authority under the warrant:

(a) cause the chief officer of the other agency to be informed forthwith of the revocation; and

(b) cause a copy of the instrument of revocation to be given as soon as practicable to the chief officer of the other agency.

121 What happens when stored communications warrants are issued

The chief officer of the agency must cause:

(a) the Managing Director of the carrier that holds the stored communications to which the warrant relates to be informed forthwith of the issue of the warrant; and

(b) a copy of the warrant, certified in writing by a certifying officer of the agency to be a true copy of the warrant, to be given as soon as practicable to the Managing Director of that carrier.

122 Revocation of stored communications warrants by chief officers

(1) The chief officer of an enforcement agency to which a stored communications warrant has been issued must, on being satisfied that the grounds on which the warrant was issued have ceased to exist:

(a) cause the chief officer of any other enforcement agency that is exercising authority under the warrant to be informed forthwith of the proposed revocation of the warrant; and

(b) by writing signed by him or her, revoke the warrant.

(2) The chief officer of an enforcement agency may at any time, by writing signed by him or her, revoke a warrant issued to the agency after causing the chief officer of any other enforcement agency that is exercising authority under the warrant to be informed forthwith that the chief officer proposes to revoke the warrant.

(3) The chief officer of an enforcement agency may delegate his or her power under subsection (2) to a certifying officer of the agency.

(4) This section does not apply in relation to a warrant that has ceased to be in force.

123 What happens when stored communications warrants are revoked

(1) Upon revoking a stored communications warrant, the chief officer of an enforcement agency must cause the chief officer of any other enforcement agency that is exercising authority under the warrant to be informed forthwith of the revocation.

(2) If the Managing Director of a carrier has been informed, under section 121, of the issue of a stored communications warrant and that warrant is subsequently revoked, the chief officer of the enforcement agency to which the warrant was issued must:

(a) cause the Managing Director of the carrier to be informed forthwith of the revocation; and

(b) cause a copy of the instrument of revocation, certified in writing by a certifying person to be a true copy of the instrument, to be given as soon as practicable to the Managing Director.

124 Access to additional telecommunications services under stored communications warrants

(1) If:

(a) the Managing Director of a carrier has been informed, under section 121, of the issue of a stored communications warrant; and

(b) it is proposed, under the warrant, to access stored communications that, immediately before they became stored communications, had passed over a telecommunications service operated by a carrier; and

(c) the service was not identified in the warrant;

the chief officer must cause the Managing Director of the carrier to be given, as soon as practicable, a description in writing of the service sufficient to identify it.

(2) If:

(a) the Managing Director of a carrier has been informed, under subsection (1) of the issue of a stored communications warrant; and

(b) the chief officer of the agency to which the warrant was issued, or a certifying officer of that agency, is satisfied that it is no longer necessary to access stored communications that, immediately before they became stored communications, had passed over that service;

the chief officer or the certifying officer must cause:

(c) the Managing Director to be informed forthwith of the fact; and

(d) confirmation in writing of the fact to be given as soon as practicable to the Managing Director.

Division 4—Provisions relating to execution of warrants

125 Entry into force of stored communications warrants

A stored communications warrant comes into force when it is issued.

126 Limit on authority conferred by warrant

A stored communications warrant does not authorise access to stored communications unless notification of the issue of the warrant has been received under section 121 by or on behalf of the Managing Director of the carrier holding the stored communications.

127 Exercise of authority conferred by warrant

(1) The authority conferred by a stored communications warrant must not be exercised by a person who is not an officer or staff member of an enforcement agency in relation to whom an approval under subsection (2) is in force in relation to the warrant.

(2) The chief officer of an agency, or an officer of an agency in relation to whom an appointment under subsection (3) is in force, may approve any of the following to exercise the authority conferred by warrants, or classes of warrants, issued to the agency:

(a) officers or staff members of the agency;

(b) classes of officers or staff members of the agency;

(c) officers or staff members of another enforcement agency;

(d) classes of officers or staff members of another enforcement agency.

(3) The chief officer of an enforcement agency may appoint in writing an officer of the agency to be an approving officer for the purposes of subsection (2).

128 Provision of technical assistance

(1) Despite subsection 127(1), a designated officer, or an employee of a carrier, may provide technical assistance to an officer or staff member of an enforcement agency who is exercising the authority conferred by a stored communications warrant.

(2) For the purposes of subsection (1), the provision of technical assistance includes (but is not limited to):

(a) the doing of any act in connection with:

(i) the installation of equipment for the purposes of accessing stored communications in accordance with a stored communications warrant; or

(ii) the maintenance, testing or use of such equipment; or

(iii) the removal of such equipment; and

(b) the doing of any act involved in the accessing of a stored communication under a stored communications warrant, to the extent that the act is incidental to the doing of an act referred to in paragraph (a).

(3) The chief officer of an enforcement agency or a person who is an approving officer for an enforcement agency under subsection 127(3) may, in writing, declare persons to be designated officers for the purposes of this section.

129 Evidentiary certificates relating to actions by carriers

(1) The Managing Director or secretary of:

(a) a carrier; or

(b) a body corporate of which the carrier is a subsidiary;

may issue a written certificate signed by him or her setting out such facts as he or she considers relevant with respect to acts or things done by, or in relation to, employees of the carrier in order to enable a warrant to be executed.

(2) A document purporting to be a certificate issued under subsection (1) and purporting to be signed by the Managing Director or secretary of a carrier, or of a body corporate of which the carrier is a subsidiary:

(a) is to be received in evidence in an exempt proceeding without further proof; and

(b) in an exempt proceeding, is conclusive evidence of the matters stated in the document.

(3) For the purposes of this section, the question whether a body corporate is a subsidiary of another body corporate is to be determined in the same manner as the question is determined under the *Corporations Act 2001*.

130 Evidentiary certificates relating to actions by enforcement agencies

(1) A certifying officer of an enforcement agency may issue a written certificate signed by him or her setting out such facts as he or she considers relevant with respect to:

(a) anything done by an officer or staff member of the agency in connection with the execution of a stored communications warrant; or

(b) anything done by an officer or staff member of the agency in connection with:

(i) the communication by a person to another person of information obtained by the execution of such a warrant; or

(ii) the making use of such information; or

(iii) the making of a record of such information; or

(iv) the custody of a record of such information; or

(v) the giving in evidence of such information.

(2) A document purporting to be a certificate issued under this section by a certifying officer of an enforcement agency and to be signed by him or her:

(a) is to be received in evidence in an exempt proceeding without further proof; and

(b) in an exempt proceeding, is *prima facie* evidence of the matters stated in the document.

131 Certified copies of stored communications warrants

A document certified in writing by a certifying officer of an enforcement agency to be a true copy of a stored communications warrant is to be received in evidence in an exempt proceeding as if it were the original warrant.

132 Obstruction

(1) A person commits an offence if the person obstructs or hinders another person acting under a stored communications warrant.

Penalty: Imprisonment for 6 months or 30 penalty units, or both.

(2) Subsection (1) does not apply if the person obstructing or hindering has a reasonable excuse.

Note: A defendant bears an evidential burden in relation to the matter in subsection (2) (see subsection 13.3(3) of the *Criminal Code*).

Part 3-4—Dealing with accessed information etc.

Division 1—Prohibition on dealing with accessed information

133 No dealing with accessed information or stored communications warrant information

(1) A person commits an offence if:

(a) the person:

(i) communicates information to another person; or

(ii) makes use of information; or

(iii) makes a record of information; or

(iv) gives information in evidence in a proceeding; and

(b) the information is:

(i) lawfully accessed information; or

(ii) information obtained by accessing a stored communication in contravention of subsection 108(1); or

(iii) stored communications warrant information.

Penalty: Imprisonment for 2 years or 120 penalty units, or both.

(2) Subsection (1) does not apply to conduct permitted under this Part.

Note 1: A defendant bears an evidential burden in relation to the matter in subsection (2) (see subsection 13.3(3) of the *Criminal Code*).

Note 2: The civil remedy provisions in Part 3-7 may apply to a contravention of this section.

Division 2—Permitted dealings with accessed information

134 Dealing in stored communications warrant information for the purposes of Part 3-2, 3-3, 3-5 or 3-6

A person may, for the purposes of Part 3-2, 3-3, 3-5 or 3-6:

(a) communicate stored communications warrant information to another person; or

(b) make use of stored communications warrant information; or

(c) make a record of stored communications warrant information; or

(d) give stored communications warrant information in evidence in a proceeding.

135 Dealing in information by employees of carriers

Communicating information to the appropriate enforcement agency

(1) An employee of a carrier may communicate information obtained by accessing stored communications under a stored communications warrant to:

(a) the officer of the enforcement agency who applied for the warrant on the agency's behalf; or

(b) an officer of the agency in relation to whom an authorisation under subsection (2) by the chief officer of the agency is in force in relation to the warrant.

(2) The chief officer of an enforcement agency may authorise in writing officers, or classes of officers, of the agency to receive information obtained by accessing stored communications under stored communications warrants, or classes of such warrants, issued to the agency.

Information relating to operation of networks etc.

(3) An employee of a carrier may communicate or make use of, or cause to be communicated, lawfully accessed information or information that has been obtained by accessing a stored communication in contravention of subsection 108(1) if:

(a) the employee does so in the performance of his or her duties as such an employee; and

(b) the information relates to:

(i) the operation or maintenance of a telecommunications network operated by the carrier; or

(ii) the supply of services by the carrier by means of a telecommunications network.

(4) An employee of a carrier may communicate or cause to be communicated to another carrier, or to an employee of another carrier, lawfully accessed information or information that has been obtained by accessing a stored communication in contravention of subsection 108(1) if:

(a) the communication of the information is for the purpose of the carrying on by the other carrier of its business relating to the supply of services by means of a telecommunications network operated by the other carrier; and

(b) the information relates to:

(i) the operation or maintenance of a telecommunications network operated by the other carrier; or

(ii) the supply of services by the other carrier by means of a telecommunications network.

Stored communications warrant information

(5) An employee of a carrier may, in the performance of his or her duties as such an employee, communicate or make use of, or cause to be communicated, stored communications warrant information if:

(a) the employee does so in the performance of his or her duties as such an employee; and

(b) the information is reasonably necessary to enable access to a stored communication under a stored communications warrant.

(6) An employee of a carrier may communicate or cause to be communicated to another carrier, or to an employee of another carrier, stored communications warrant information if the information is reasonably necessary to enable access to a stored communication under a stored communications warrant.

136 Dealing in connection with Organisation's functions

(1) A person may, in connection with the performance by the Organisation of its functions, or otherwise for purposes of security, communicate to another person, make use of, or make a record of the following:

(a) lawfully accessed information other than foreign intelligence information;

(b) stored communications warrant information.

(2) The Director-General of Security may, in connection with the performance by the Organisation of its functions, communicate foreign intelligence information to an officer or employee of the Organisation.

(3) An officer or employee of the Organisation may, in connection with the performance by the Organisation of its functions, communicate foreign intelligence information to the Director-General of Security or to another such officer or employee.

(4) The Director-General of Security or an officer or employee of the Organisation may, in connection with the performance by the Organisation of its functions, make use of, or make a record of, foreign intelligence information.

137 Communicating information obtained by Organisation

(1) The Director-General of Security may, in accordance with paragraph 18(3)(a) or (b) of the *Australian Security Intelligence Organisation Act 1979*, communicate the following to another person:

(a) lawfully accessed information;

(b) stored communications warrant information.

(2) The communication may be made by the Director-General of Security personally or by a person authorised by the Director-General.

(3) A person to whom foreign intelligence information has been communicated:

(a) in accordance with subsection (1); or

(b) in accordance with an approval given under this subsection;

may communicate that information to such persons, and in such manner, as are approved in writing by the Attorney-General.

138 Employee of carrier may communicate information to enforcement agency

(1) An employee of a carrier may, for a purpose or purposes connected with the investigation by the Australian Communications and Media Authority of a serious contravention or with the performance of its functions relating to enforcement of the *Spam Act 2003*, and for no other purpose, communicate to an officer or staff member of the authority the following:

(a) lawfully accessed information other than foreign intelligence information;

(b) stored communications warrant information.

(2) An employee of a carrier may, for a purpose or purposes connected with the investigation by any other enforcement agency of a serious contravention, and for no other purpose, communicate to an officer or staff member of the agency the following:

(a) lawfully accessed information other than foreign intelligence information;

(b) stored communications warrant information.

139 Dealing for purposes of investigation etc.

(1) An officer or staff member of an enforcement agency or an eligible Commonwealth authority may, for one or more purposes referred to in subsection (2), and for no other purpose, communicate to another person, make use of, or make a record of the following:

(a) lawfully accessed information other than foreign intelligence information;

(b) stored communications warrant information.

(2) The purposes are purposes connected with:

(a) an investigation by the agency of a contravention to which subsection (3) applies; or

(b) the making by an authority, body or person of a decision whether or not to begin a proceeding to which subsection (4) applies; or

(c) a proceeding to which subsection (4) applies; or

(d) the keeping of records by the agency under Part 3-5.

(3) A contravention to which this subsection applies is a contravention of a law of the Commonwealth, a State or a Territory that:

(a) is a serious offence; or

(b) is an offence punishable:

(i) by imprisonment for a period, or a maximum period, of at least 12 months; or

(ii) if the offence is committed by an individual—by a fine, or a maximum fine, of at least 60 penalty units; or

(iii) if the offence cannot be committed by an individual—by a fine, or a maximum fine, of at least 300 penalty units; or

(c) could, if established, render the person committing the contravention liable:

(i) if the contravention were committed by an individual—to pay a pecuniary penalty of 60 penalty units or more, or to pay an amount that is the monetary equivalent of 60 penalty units or more; or

(ii) if the contravention cannot be committed by an individual—to pay a pecuniary penalty of 300 penalty units or more, or to pay an amount that is the monetary equivalent of 300 penalty units or more.

(4) A proceeding to which this subsection applies is:

(a) a proceeding by way of a prosecution for an offence of a kind referred to in paragraph (3)(a) or (b); or

(b) a proceeding for the confiscation or forfeiture of property, or for the imposition of a pecuniary penalty, in connection with the commission of such an offence; or

(c) a proceeding for the taking of evidence pursuant to section 43 of the *Extradition Act 1988*, in so far as the proceeding relates to such an offence; or

(d) a proceeding for the extradition of a person from a State or a Territory to another State or Territory, in so far as the proceeding relates to such an offence; or

(e) a proceeding for recovery of a pecuniary penalty for a contravention of a kind referred to in paragraph (3)(c).

(5) To avoid doubt, a reference in subsection (3) to a number of penalty units in relation to a contravention of a law of a State or a Territory includes a reference to an amount of a fine or pecuniary penalty that is equivalent, under section 4AA of the *Crimes Act 1914*, to that number of penalty units.

140 Dealing with information if access suspected to be unlawful

(1) A person may communicate information to the Attorney-General, the Director of Public Prosecutions, the Commissioner of Police or the Chief Executive Officer of the ACC if:

(a) the information was obtained by accessing a stored communication; and

(b) the person suspects on reasonable grounds that the information may tend to establish that an offence of the following kind (a ***suspected offence***) has been committed:

(i) an offence against subsection 108(1) constituted by the access, or by authorising, suffering or permitting, or doing an act or thing to enable, the access;

(ii) an offence against section 133 constituted by communicating to a person, making use of, making a record of, or giving in evidence in a proceeding, information obtained by the access;

(iii) an ancillary offence relating to an offence of a kind referred to in subparagraph (i) or (ii) of this paragraph.

(2) A person to whom the information is communicated in accordance with subsection (1) may communicate to another person, make use of, or make a record of, some or all of the information for a purpose (or 2 or more purposes) connected with:

(a) an investigation of a suspected offence; or

(b) the making by an authority, body or person of a decision whether or not to begin a proceeding by way of a prosecution for a suspected offence; or

(c) a proceeding by way of a prosecution for a suspected offence;

and for no other purpose.

141 Making record for purpose of permitted communication

A person who is permitted by section 135, 137 or 138 or subsection 140(1) to communicate particular information to another person may:

(a) make a record of the information, or

(b) cause such a record to be made;

for the purpose of so communicating the information in accordance with that section or subsection.

142 Further dealing by recipient of certain information

A person to whom information has, in accordance with subsection 135(4), section 139, subsection 140(2) or this section, been communicated for a purpose, or for 2 or more purposes, may:

(a) communicate that information to another person; or

(b) make use of, or make a record of, that information;

for that purpose, or for one or more of those purposes, and for no other purpose.

143 Giving information in evidence in exempt proceeding

(1) A person may give lawfully accessed information (other than foreign intelligence information) in evidence in an exempt proceeding.

(2) For the purposes of applying subsection (1) in relation to information, the question whether or not a stored communication

was accessed in contravention of subsection 108(1) may be determined on the balance of probabilities.

(3) A person may give stored communications warrant information in evidence in an exempt proceeding.

144 Giving information in evidence if communication unlawfully accessed

(1) A person may give, in evidence in an exempt proceeding, information obtained by accessing stored communications obtained in contravention of subsection 108(1) if:

(a) the access was purportedly under a stored communications warrant; and

(b) the court in which, or the tribunal, body, authority or person before which, the proceeding is held is satisfied that:

(i) but for an irregularity, the access would not have constituted a contravention of subsection 108(1); and

(ii) the irregularity is not a substantial defect or irregularity; and

(iii) in all the circumstances, the irregularity should be disregarded.

(2) A reference in subsection (1) to an irregularity is a reference to a defect or irregularity:

(a) in, or in connection with the issue of, a document purporting to be a warrant; or

(b) in connection with the execution of a warrant, or the purported execution of a document purporting to be a warrant.

145 Evidence that has been given in exempt proceeding

If information is given in evidence in an exempt proceeding under section 143 or 144, that information, or any part of that information, may later be given in evidence in any proceeding.

Note: This section was inserted as a response to the decision of the Court of Appeal of New South Wales in *Wood v Beves* (1997) 92 A Crim R 209.

146 Giving information in evidence in civil proceedings for remedial relief

(1) A person may give information obtained by accessing a stored communication in contravention of subsection 108(1) in evidence in a proceeding by way of an application under section 165 for remedial relief in respect of:

(a) the access; or

(b) the communication (in contravention of section 133) of information obtained by the access.

(2) A person may give stored communications warrant information in evidence in a proceeding by way of an application under section 165.

Division 3—Admissibility of evidence

147 Accessed material inadmissible except as provided

(1) Neither information, nor a record, obtained by accessing a stored communication is admissible in evidence in a proceeding except in so far as section 143, 144, 145 or 146 permits a person to give in evidence in that proceeding information so obtained.

(2) Subsection (1) of this section applies whether or not the stored communication was accessed in contravention of subsection 108(1).

(3) However, for the purpose of determining the extent (if any) to which section 143, 144, 145 or 146 permits a person to give in evidence in a proceeding information obtained by the access:

(a) a person may communicate to another person, make use of, make a record of, or give in evidence in the last-mentioned proceeding, information so obtained; and

(b) information, or a record, so obtained is admissible in evidence in the last-mentioned proceeding.

148 Stored communications warrant information inadmissible except as provided

(1) Stored communications warrant information is admissible in evidence in a proceeding only to the extent that section 143, 145 or

146 permits a person to give stored communications warrant information in evidence in that proceeding.

(2) For the purpose of determining the extent (if any) to which section 143, 145 or 146 permits a person to give stored communications warrant information in evidence in a proceeding:

(a) a person may:

(i) communicate the information to another person; or

(ii) make use of the information; or

(iii) make a record of the information; or

(iv) give the information in evidence in the proceeding; and

(b) the information is admissible in evidence in the proceeding.

149 Evidence that is otherwise inadmissible

This Part does not render:

(a) information; or

(b) any record that was obtained by accessing a stored communication (whether or not in contravention of subsection 108(1));

admissible in evidence in a proceeding to a greater extent than it would have been admissible in evidence in that proceeding if this Part had not been enacted.

Division 4—Destruction of records

150 Destruction of records

(1) If:

(a) information, or a record, that was obtained by accessing a stored communication (whether or not in contravention of subsection 108(1)) is in an enforcement agency's possession; and

(b) the chief officer of the agency is satisfied that the information or record is not likely to be required for a purpose referred to in subsection 139(2);

the chief officer must cause the information or record to be destroyed forthwith.

(2) The chief officer must, as soon as practicable, and in any event within 3 months, after each 30 June, give to the Minister a written report that sets out the extent to which information and records were destroyed in accordance with this section.

Part 3-5—Keeping and inspection of access records

Division 1—Keeping access records

151 Enforcement agencies to keep documents connected with issue of warrants

The chief officer of an enforcement agency must cause to be kept in the agency's records:

(a) each stored communications warrant issued to the agency; and

(b) each instrument revoking such a warrant; and

(c) a copy of each certificate issued under subsection 130(1) by a certifying officer of the agency; and

(d) each authorisation by the chief officer under subsection 135(2); and

(e) particulars of the destruction of information and records that the chief officer has caused in accordance with section 150.

Division 2—Inspection of access records by Ombudsman

152 Functions of Ombudsman

Subject to this Division, the Ombudsman has the following additional functions:

(a) to inspect an enforcement agency's records in order to ascertain, so far as is practicable, the extent of compliance, in relation to those records, with sections 150 and 151; and

(b) to report to the Minister about the results of inspections under this Division; and

(c) to do anything incidental or conducive to the performance of any of the preceding functions.

153 Reports

(1) The Ombudsman must report to the Minister in writing, in relation to each enforcement agency, about the results of the inspections under section 152, during that financial year, of the agency's records.

(2) Each report under subsection (1) in relation to a financial year must be given to the Minister as soon as practicable after the end of the financial year, and in any event within 3 months after the end of the financial year.

(3) If, as a result of an inspection under this Division of the records of an enforcement agency, the Ombudsman is of the opinion that an officer of the agency has contravened a provision of this Act (other than section 150 or 151), the Ombudsman may include in his or her report on the inspection a report on the contravention.

Note: In complying with this section, the Ombudsman remains bound by the obligations imposed by section 133 relating to disclosure of accessed information or stored communications warrant information.

(4) The Ombudsman may report to the Minister in writing at any time about the results of an inspection under this Division and must do so if so requested by the Minister.

(5) The Ombudsman must give a copy of a report under subsection (1) or (3) to the chief officer of the enforcement agency to which the report relates.

154 Ombudsman's general powers

(1) Subject to section 133, the Ombudsman's powers under the *Ombudsman Act 1976* extend to an inspection by the Ombudsman under this Division as if the inspection were an investigation by the Ombudsman under that Act.

(2) The exercise of those powers in relation to an inspection by the Ombudsman under this Division is taken, for all purposes, to be an exercise of powers under the *Ombudsman Act 1976*.

155 Ombudsman to be given information etc. despite other laws

(1) Neither section 133 nor any other law prevents an officer of an enforcement agency from:

(a) giving information to an inspecting officer (whether orally or in writing and whether or not in answer to a question); or

(b) giving to an inspecting officer access to a record of the agency;

for the purposes of an inspection under this Part of the agency's records.

(2) Neither section 133 nor any other law prevents an officer of an enforcement agency from making a record of information, or causing a record of information to be made, for the purposes of giving the information to a person as permitted by subsection (1).

156 Dealing with information for the purposes of inspection and report

(1) An inspecting officer may communicate to another inspecting officer, make use of, or make a record of, information for the purposes of an inspection (or of a report on an inspection) under this Division of an enforcement agency's records if:

(a) the information was given or communicated to the inspecting officer, as permitted by subsection 155(1) or this section, for the purposes of an inspection (or of a report on an inspection) under this Division of an enforcement agency's records; or

(b) the inspecting officer obtained the information as a result of being given access to records of an enforcement agency, as permitted by subsection 155(1), for the purposes of an inspection under this Division of the agency's records.

(2) This section has effect despite section 133 or any other law.

157 Application of Ombudsman Act

(1) Section 11A of the *Ombudsman Act 1976* does not apply in relation to the exercise or proposed exercise of a power, or the performance or the proposed performance of a function, of the Ombudsman under this Division.

(2) A reference in section 19 of the *Ombudsman Act 1976* to the Ombudsman's operations does not include a reference to anything that an inspecting officer has done or omitted to do under this Division.

(3) Subject to section 155 of this Act, subsections 35(2), (3), (4) and (8) of the *Ombudsman Act 1976* apply for the purposes of this Division and so apply as if:

(a) a reference in those subsections to an officer were a reference to an inspecting officer; and

(b) a reference in those subsections to information did not include a reference to lawfully accessed information or lawfully intercepted information; and

(c) a reference in those subsections to that Act were a reference to this Division; and

(d) paragraph 35(3)(b) of that Act were omitted; and

(e) section 35A of that Act had not been enacted.

158 Exchange of information between Ombudsman and State inspecting authorities

(1) The Ombudsman may give information that:

(a) relates to an enforcement agency that is an authority of a State (a ***State agency***); and

(b) was obtained by the Ombudsman under this Act;

to the authority (a ***State inspecting authority***) that, under the law of the State concerned, has the function of making inspections of the kind referred to in paragraph 35(1)(h) in relation to the agency.

(2) The Ombudsman may give information to an authority under subsection (1) only if the Ombudsman is satisfied that the giving of the information is necessary to enable the authority to perform its functions in relation to the State agency.

(3) The Ombudsman may receive from a State inspecting authority information relevant to the performance of the Ombudsman's functions under this Act.

Part 3-6—Reports about access to stored communications

Division 1—Reports to the Minister

159 Annual reports regarding applications and warrants under Part 3-3

(1) The chief officer of an enforcement agency must, as soon as practicable, and in any event within 3 months, after each 30 June, give to the Minister a written report that sets out such information as:

(a) Division 2 requires to be set out in the Minister's report under that Division relating to the year ending on that 30 June; and

(b) can be derived from the agency's records.

(2) Section 34C of the *Acts Interpretation Act 1901* does not apply in relation to a report under this section.

160 Minister may seek further information from Commonwealth agency

(1) The Minister may, by writing, request the chief officer of an enforcement agency to give to the Minister in writing specified information that:

(a) the Minister needs in connection with preparing a report under Division 2; and

(b) is not contained in a report by the chief officer under section 159.

(2) To the extent that it is practicable to do so, the chief officer must comply with the request.

Division 2—Reports by the Minister

161 Annual report by Minister about stored communications warrants

The Minister must, as soon as practicable after each 30 June, cause to be prepared a written report that relates to the year ending on that 30 June and complies with this Division.

162 Report to set out how many applications made and warrants issued

(1) The report must set out, for each enforcement agency:
  (a) the relevant statistics about applications for stored communications warrants that the agency made during that year; and
  (b) the relevant statistics about telephone applications for stored communications warrants that the agency made during that year.

(2) The report must set out:
  (a) the relevant statistics about applications for stored communications warrants that were made during that year; and
  (b) the relevant statistics about telephone applications for stored communications warrants that were made during that year; and
  (c) the relevant statistics about renewal applications made during that year; and
  (d) how many stored communications warrants issued on applications made during that year specified conditions or restrictions relating to access to stored communications under the warrants.

163 Report to contain information about effectiveness of warrants

The report must set out, for each enforcement agency:
  (a) how many arrests were made during that year on the basis of information that was, or included, lawfully accessed information; and

(b) how many proceedings ended during that year that were proceedings in which, according to the records of the agency, lawfully accessed information was given in evidence.

Division 3—Provisions about annual reports

164 Annual reports

(1) The Minister must cause a copy of a report under Division 2 to be laid before each House of the Parliament within 15 sitting days of that House after the report is prepared.

(2) A report under Division 2 must not be made in a manner that is likely to enable the identification of a person.

(3) For the purposes of section 34C of the *Acts Interpretation Act 1901*, a report that Division 2 requires to be prepared as soon as practicable after 30 June in a calendar year is taken to be a periodic report:
(a) that this Act requires a person to give to the Minister; and
(b) that relates to the administration of Parts 3-3, 3-4 and 3-5 during the year ending on that 30 June.

Part 3-7—Civil remedies

165 Civil remedies—unlawful access or communication

When section applies

(1) This section applies to an accessing of a stored communication if the access was in contravention of subsection 108(1).

Aggrieved person

(2) For the purposes of this section, a person is an ***aggrieved person*** if, and only if:
(a) the person was a party to the communication; or
(b) the communication was made on the person's behalf.

Access—civil court remedy

(3) If a person (the ***defendant***):

(a) so accessed the communication; or

(b) did an act or thing referred to in subparagraph 108(1)(a)(ii) or (iii) in relation to the access;

the Federal Court of Australia or a court of a State or Territory may, on the application of an aggrieved person, grant the aggrieved person remedial relief in respect of the access by making such orders against the defendant as the court considers appropriate.

Note: Subparagraphs 108(1)(a)(ii) and (iii) deal with the authorisation or enabling of access etc.

Communication—civil court remedy

(4) If:

(a) information was obtained by accessing the communication; and

(b) a person (the ***defendant***) communicated the information to another person in contravention of section 133;

the Federal Court of Australia or a court of a State or Territory may, on the application of an aggrieved person, grant the aggrieved person remedial relief in respect of the communication of the information by making such orders against the defendant as the court considers appropriate.

Access—criminal court remedy

(5) If a court convicts a person (the ***defendant***) of an offence against subsection 108(1) constituted by:

(a) the access; or

(b) the doing of an act or thing referred to in subparagraph 108(1)(a)(ii) or (iii) in relation to the access;

the court may, on the application of an aggrieved person, grant the aggrieved person remedial relief in respect of the access by making such orders against the defendant as the court considers appropriate.

Note: Subparagraphs 108(1)(a)(ii) and (iii) deal with the authorisation or enabling of access etc.

Communication—criminal court remedy

(6) If:

(a) information was obtained by accessing the communication; and

(b) the information was communicated to a person in contravention of section 133; and

(c) a court convicts a person (in this subsection called the ***defendant***) of an offence against section 133 constituted by the communication of the information;

the court may, on the application of an aggrieved person, grant the aggrieved person remedial relief in respect of the communication of the information by making such orders against the defendant as the court considers appropriate.

Orders

(7) Without limiting the orders that may be made under this section against a person (the ***defendant***) in respect of a particular access to or a particular communication of information, a court may make an order of one or more of the following kinds:

(a) an order declaring the access or communication, as the case requires, to have been unlawful;

(b) an order that the defendant pay to the aggrieved person such damages as the court considers appropriate;

(c) an order in the nature of an injunction (including a mandatory injunction);

(d) an order that the defendant pay to the aggrieved person an amount not exceeding the amount that, in the opinion of the court, represents the total gross income derived by the defendant as a result of the access or communication, as the case requires.

Terms etc. of orders

(8) Without limiting the orders that may be made by a court under this section, an order may:

(a) include such provisions as the court considers necessary for the purposes of the order; and

(b) be made either unconditionally or subject to such terms and conditions as the court determines.

Injunctive relief—variation etc.

(9) A court may revoke or vary an order in the nature of an injunction made by the court under this section.

Punitive damages

(10) A reference in paragraph (7)(b) to damages includes a reference to damages in the nature of punitive damages.

Minor irregularities in warrants etc.

(11) Despite subsection (1) of this section, this section does not apply to an accessing that contravenes subsection 108(1) only because of a defect or irregularity (other than a substantial defect or irregularity):

(a) in, or in connection with the issue of, a document purporting to be a warrant; or

(b) in connection with the execution of a warrant, or the purported execution of a document purporting to be a warrant.

166 Limitation periods etc.

Access—civil court remedy

(1) An application under subsection 165(3) for the grant of remedial relief in respect of an access is to be made within 6 years after the access took place.

Communication—civil court remedy

(2) An application under subsection 165(4) for the grant of remedial relief in respect of a communication of information is to be made within 6 years after the communication.

Criminal court remedies

(3) An application under subsection 165(5) or (6) for the grant of remedial relief is not subject to any limitation period, but is to be made as soon as practicable after the conviction concerned.

167 No limitation on other liability

No limitation

(1) This Part does not limit any liability (whether criminal or civil) that a person has under any other provision of this Act or under any other law.

Remedial relief even if defendant convicted of offence

(2) An application under subsection 165(3) or (4) may be made even if the defendant referred to in that subsection has been convicted of an offence under, or arising out of, this Act.

168 Concurrent operation of State and Territory laws

This Part is not intended to exclude or limit the operation of a law of a State or Territory that is capable of operating concurrently with this Part.

169 State or Territory courts—jurisdictional limits

This Part does not enable an inferior court of a State or Territory to grant remedial relief of a kind that the court is unable to grant under the law of that State or Territory.

170 Extended meaning of *conviction*—orders under section 19B of the *Crimes Act 1914*

A reference in this Part to the conviction of a person of an offence includes a reference to the making of an order under section 19B of the *Crimes Act 1914* in relation to a person in respect of an offence.

Note: Section 19B of the *Crimes Act 1914* empowers a court that has found a person to have committed an offence to take action without proceeding to record a conviction.

Part 2—Other amendments

Administrative Decisions (Judicial Review) Act 1977

10 Paragraph (d) of Schedule 1

Omit "*Telecommunications (Interception) Act 1979*", substitute "*Telecommunications (Interception and Access) Act 1979*".

Australian Crime Commission Act 2002

11 Subsection 19A(5)

Omit "section 63 of the *Telecommunications (Interception) Act 1979*", substitute "sections 63 and 133 of the *Telecommunications (Interception and Access) Act 1979*".

12 Schedule 1

Omit "*Telecommunications (Interception) Act 1979*, section 63", substitute "*Telecommunications (Interception and Access) Act 1979*, sections 63 and 133".

Australian Security Intelligence Organisation Act 1979

13 Paragraph 17(1)(e)

Omit "*Telecommunications (Interception) Act 1979*" (wherever occurring), substitute "*Telecommunications (Interception and Access) Act 1979*".

14 Subsection 26(8)

Omit "*Telecommunications (Interception) Act 1979*", substitute "*Telecommunications (Interception and Access) Act 1979*".

15 Subsection 27A(5)

Omit "*Telecommunications (Interception) Act 1979*", substitute "*Telecommunications (Interception and Access) Act 1979*".

Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Act (No. 2) 2004

16 Subitems 31(1) and (2) of Schedule 1

Omit "*Telecommunications (Interception) Act 1979*", substitute "*Telecommunications (Interception and Access) Act 1979*".

Criminal Code Act 1995

17 Section 473.1 of the *Criminal Code* (definition of *interception device*)

Omit "*Telecommunications (Interception) Act 1979*", substitute "*Telecommunications (Interception and Access) Act 1979*".

18 Subsection 474.4(2) of the *Criminal Code*

Omit "*Telecommunications (Interception) Act 1979*", substitute "*Telecommunications (Interception and Access) Act 1979*".

19 Paragraph 476.5(2A)(a) of the *Criminal Code*

Omit "Part III of the *Telecommunications (Interception) Act 1979*", substitute "Part 2-2 of the *Telecommunications (Interception and Access) Act 1979*".

Freedom of Information Act 1982

20 Schedule 3

Omit "*Telecommunications (Interception) Act 1979*, section 63", substitute "*Telecommunications (Interception and Access) Act 1979*, sections 63 and 133".

Intelligence Services Act 2001

20A Paragraph 14(2A)(a)

Omit "Part III of the *Telecommunications (Interception) Act 1979*", substitute "Part 2-2 of the *Telecommunications (Interception and Access) Act 1979*".

Law Officers Act 1964

21 Subsection 17(6)

Omit "*Telecommunications (Interception) Act 1979*", substitute "*Telecommunications (Interception and Access) Act 1979*".

Mutual Assistance in Criminal Matters Act 1987

22 Subsection 13A(6) (definition of *material lawfully obtained by an enforcement agency in Australia*)

Omit "*Telecommunications (Interception) Act 1979*", substitute "*Telecommunications (Interception and Access) Act 1979*".

Surveillance Devices Act 2004

23 Subsection 18(7)

Omit "*Telecommunications (Interception) Act 1979*", substitute "*Telecommunications (Interception and Access) Act 1979*".

24 Subsection 32(4)

Omit "*Telecommunications (Interception) Act 1979*", substitute "*Telecommunications (Interception and Access) Act 1979*".

Telecommunications Act 1997

24A Section 5

Omit "*Telecommunications (Interception) Act 1979*", substitute "*Telecommunications (Interception and Access) Act 1979*".

24B Subsection 313(7)

Omit "interception services", substitute "interception or access services".

24C Subsection 313(7)

Omit "under the *Telecommunications (Interception) Act 1979*", substitute "or a stored communications warrant under the *Telecommunications (Interception and Access) Act 1979*".

24D Subsection 313(8)

Omit "interception services", substitute "interception or access services".

24E Subsection 313(8)

After "intercepted", insert "or accessed".

24F Subsection 324(2)

Omit "*Telecommunications (Interception) Act 1979*", substitute "*Telecommunications (Interception and Access) Act 1979*".

24G Section 332K (note)

Omit "*Telecommunications (Interception) Act 1979*", substitute "*Telecommunications (Interception and Access) Act 1979*".

Telecommunications (Interception) Act 1979

25 Title

After "**interception of**", insert "**, and other access to,**".

26 Part I (heading)

Repeal the heading, substitute:

Chapter 1—Introduction

Part 1-1—Preliminary

27 Section 1

After "*Interception*", insert "*and Access*".

28 Part IA (heading)

Repeal the heading, substitute:

Part 1-2—Interpretation

29 Subsection 5(1)

Insert:

access, in relation to a stored communication, has the meaning given by section 6AA.

30 Subsection 5(1)

Insert:

accessible, in relation to a communication, has the meaning given by section 5H.

31 Subsection 5(1) (definition of *agency*)

Repeal the definition, substitute:

agency means:

(a) except in Chapter 2—an interception agency or another enforcement agency; or

(b) in Chapter 2—an interception agency.

32 Subsection 5(1) (at the end of the definition of *certifying officer*)

Add:

; or (j) in the case of any other agency:

(i) the chief executive officer or an acting chief executive officer of the agency; or

(ii) an officer of the agency (by whatever name called) who holds, or is acting in, an office or position in the agency which is involved in the management of the agency and which has been nominated in writing by the chief executive officer for the purposes of this subparagraph.

33 Subsection 5(1) (at the end of the definition of *chief officer*)

Add:

; or (m) in the case of an enforcement agency that is not an interception agency and is not an eligible authority of a State—the chief executive officer or an acting chief executive officer of the agency.

34 Subsection 5(1) (definition of *designated warrant information*)

Repeal the definition.

35 Subsection 5(1)

Insert:

emergency service facility has the meaning given by subsection 6(2A).

36 Subsection 5(1)

Insert:

enforcement agency has the same meaning as in section 282 of the *Telecommunications Act 1997*, and includes an interception agency and an eligible authority of a State.

37 Subsection 5(1) (definition of *foreign communications warrant*)

Omit "a warrant", substitute "an interception warrant".

38 Subsection 5(1)

Insert:

intended recipient, of a communication, has the meaning given by section 5G.

39 Subsection 5(1)

Insert:

interception agency means:

(a) except for the purposes of Part 2-6:

(i) a Commonwealth agency; or
(ii) an eligible authority of a State in relation to which a declaration under section 34 is in force; or

(b) for the purposes of Part 2-6:
(i) a Commonwealth agency; or
(ii) an eligible authority of a State.

40 Subsection 5(1)

Insert:

interception warrant means a warrant issued under Chapter 2.

41 Subsection 5(1)

Insert:

interception warrant information has the meaning given by section 6EA.

42 Subsection 5(1)

Insert:

issuing authority means a person in respect of whom an appointment is in force under section 6DB.

43 Subsection 5(1)

Insert:

lawfully accessed information means information obtained by accessing a stored communication otherwise than in contravention of subsection 108(1).

44 Subsection 5(1)

Insert:

lawfully intercepted information has the meaning given by section 6E.

45 Subsection 5(1)

Insert:

listening device has the same meaning as in Division 2 of Part III of the *Australian Security Intelligence Organisation Act 1979*.

46 Subsection 5(1) (definition of *named person warrant*)

Omit "a warrant", substitute "an interception warrant".

47 Subsection 5(1) (definition of *nominated AAT member*)

Omit "Part VI", substitute "Part 2-5".

48 Subsection 5(1)

Insert:

Part 2-2 warrant means a warrant issued under Part 2-2.

49 Subsection 5(1)

Insert:

Part 2-5 warrant means a warrant issued under Part 2-5.

50 Subsection 5(1) (definition of *Part III warrant*)

Repeal the definition.

51 Subsection 5(1) (definition of *Part VI warrant*)

Repeal the definition.

52 Subsection 5(1) (at the end of the definition of *passing over*)

Add:

Note: See section 5F for when a communication is passing over a telecommunications system.

53 Subsection 5(1) (definition of *permitted purpose*)

Omit "an agency", substitute "an interception agency".

54 Subsection 5(1) (subparagraph (a)(v) of the definition of *permitted purpose*)

Omit "Part VIII", substitute "Part 2-7".

55 Subsection 5(1) (after paragraph (b) of the definition of *prescribed offence*)

Insert:

(ba) an offence against subsection 108(1) or section 133; or

56 Subsection 5(1)

Insert:

publicly-listed ASIO number has the meaning given by subsection 6(3).

57 Subsection 5(1)

Insert:

serious contravention has the meaning given by section 5E.

58 Subsection 5(1)

Insert:

stored communications warrant means a warrant issued under Chapter 3.

59 Subsection 5(1)

Insert:

stored communications warrant information has the meaning given by section 6EB.

60 Subsection 5(1) (definition of *telecommunications service warrant*)

Omit "a warrant", substitute "an interception warrant".

61 Subsection 5(1) (definition of *telephone application*)

Omit "Part VI warrant", substitute "Part 2-5 warrant or a stored communications warrant".

62 Subsection 5(1) (definition of *warrant*)

Repeal the definition, substitute:

warrant means:

(a) except in Chapter 2—an interception warrant or a stored communications warrant; or

(b) in Chapter 2 (except in Part 2-5)—an interception warrant (whether issued before or after the commencement of this definition); or

(c) in Part 2-5—a Part 2-5 warrant.

63 Section 5B

Before "A reference in this Act", insert "(1)".

64 At the end of section 5B

Add:

(2) Without limiting subsection (1), a reference in Chapter 3 to an exempt proceeding includes a reference to:

(a) a proceeding by way of a prosecution for an offence punishable:

(i) by imprisonment for a period, or a maximum period, of at least 12 months; or

(ii) by a fine, or a maximum fine, of at least 60 penalty units if the offence is committed by an individual; or

(iii) if the offence cannot be committed by an individual—by a fine, or a maximum fine, of at least 300 penalty units; or

(b) a proceeding for the confiscation or forfeiture of property, or for the imposition of a pecuniary penalty, in connection with the commission of such an offence; or

(c) a proceeding for the taking of evidence pursuant to section 43 of the *Extradition Act 1988*, in so far as the proceeding relates to such an offence; or

(d) a proceeding for the extradition of a person from a State or Territory to another State or Territory, in so far as the proceeding relates to such an offence; or

(e) a proceeding by way of a coroner's inquest if, in the opinion of the coroner, the event that is the subject of the inquest may have resulted from the commission of such an offence; or

(f) a proceeding for recovery of a pecuniary penalty for a contravention that would, if proved, render the person committing the contravention liable to:

(i) a pecuniary penalty, or a maximum pecuniary penalty, of at least 60 penalty units if the contravention is committed by an individual; or

(ii) if the contravention cannot be committed by an individual—a pecuniary penalty, or a maximum pecuniary penalty, of at least 300 penalty units.

65 Subsection 5C(1)

Omit "Part VIII", substitute "Part 2-7 or 3-5".

66 Subsection 6(2A)

Omit "In this section, ***emergency service facility*** means", substitute "An ***emergency service facility*** is".

67 Subsection 6(3)

Omit "In this section, a", substitute "A".

68 Subsections 6DA(1) and (4)

Omit "Part VI", substitute "Part 2-5 or 3-3".

Note: The heading to section 6DA is altered by omitting "**may issue Part VI warrants**".

69 Subsection 6E(1)

Omit "subsections (2) and (3)", substitute "subsection (2)".

70 Subsections 6E(1) and (2)

Omit "lawfully obtained information", substitute "lawfully intercepted information".

Note: The heading to section 6E is replaced by the heading "**Lawfully intercepted information**".

71 Subsection 6E(3)

Repeal the subsection.

72 Section 6EA

Omit "***designated warrant information***", substitute "***interception warrant information***".

Note: The heading to section 6EA is replaced by the heading "**Interception warrant information**".

73 Section 6EA

Omit "a warrant" (wherever occurring), substitute "an interception warrant".

74 Section 6H

Omit "Part VI" (first occurring), substitute "Part 2-5".

75 Paragraph 6H(b)

Omit "Part VI warrant", substitute "Part 2-5 warrant".

76 At the end of section 6H

Add:

; or (c) in the case of a stored communications warrant—paragraph 116(1)(d).

77 Paragraph 6L(1)(c)

Omit "paragraph 5B(c)", substitute "paragraph 5B(1)(c)".

78 Paragraph 6L(1)(d)

Omit "paragraph 5B(d)", substitute "paragraph 5B(1)(d)".

79 Part II (heading)

Repeal the heading, substitute:

Chapter 2—Interception of telecommunications

Part 2-1—Prohibition on interception of telecommunications

80 Paragraph 7(2)(ad)

Repeal the paragraph.

81 Subsections 7(3) and (3A)

Repeal the subsections.

82 Paragraphs 7(4)(c) and (5)(c)

Omit "Part VI warrant", substitute "Part 2-5 warrant".

83 Subsections 7(6) and (6A)

Omit “Part VI warrant”, substitute “Part 2-5 warrant”.

84 Paragraphs 7(10)(b) and (c)

Omit “Part VI warrant”, substitute “Part 2-5 warrant”.

85 Part III (heading)

Repeal the heading, substitute:

Part 2-2—Warrants authorising the Organisation to intercept telecommunications

86 Subsection 12(1)

Omit “Part III warrants”, substitute “Part 2-2 warrants”.

87 Section 13

Omit “Part III warrant”, substitute “Part 2-2 warrant”.

88 Paragraph 14(a)

Omit “Part III warrant”, substitute “Part 2-2 warrant”.

89 Subsection 15(1)

Omit “Part III warrant”, substitute “Part 2-2 warrant”.

90 Subsection 17(1)

Omit “Part III warrant”, substitute “Part 2-2 warrant”.

91 Part V (heading)

Repeal the heading, substitute:

Part 2-3—Emergency requests authorising officers of a carrier to intercept telecommunications

92 Part VI (heading)

Repeal the heading, substitute:

Part 2-5—Warrants authorising agencies to intercept telecommunications

93 Subparagraph 35(1)(d)(i)

Omit "Part IX", substitute "Part 2-8".

94 Paragraph 53(1)(d)

Omit "Part VI warrant", substitute "Part 2-5 warrant".

95 Subsection 55(1)

Omit "Part VI warrant", substitute "Part 2-5 warrant".

96 Paragraph 61(4)(a)

Omit "Part VI warrant", substitute "Part 2-5 warrant".

97 Part VII (heading)

Repeal the heading, substitute:

Part 2-6—Dealing with intercepted information etc.

98 Subsection 63(1)

Omit "lawfully obtained information", substitute "lawfully intercepted information".

99 Subsection 63(2)

Omit "designated warrant information" (wherever occurring), substitute "interception warrant information".

Note: The heading to section 63 is altered by omitting "**designated warrant information**" and substituting "**interception warrant information**".

100 Section 63AA

Omit "Part III, VI, VIII or IX", substitute "Part 2-2, 2-5, 2-7 or 2-8".

Note: The heading to section 63AA is replaced by the heading "**Dealing in interception warrant information for the purposes of Part 2-2, 2-5, 2-7 or 2-8**".

101 Section 63AA

Omit "designated warrant information" (wherever occurring), substitute "interception warrant information".

102 Subsections 63B(3) and (4)

Omit "designated warrant information", substitute "interception warrant information".

103 Paragraph 64(1)(a)

Omit "lawfully obtained information", substitute "lawfully intercepted information".

104 Paragraph 64(1)(b)

Repeal the paragraph, substitute:

(b) interception warrant information.

105 Paragraphs 65(1)(a) and (b)

Repeal the paragraphs, substitute:

(a) lawfully intercepted information;

(b) interception warrant information.

106 Paragraph 65A(a)

Omit "lawfully obtained information", substitute "lawfully intercepted information".

107 Paragraph 65A(b)

Repeal the paragraph, substitute:

(b) interception warrant information.

108 Paragraph 67(1)(a)

Omit "lawfully obtained information", substitute "lawfully intercepted information".

109 Paragraph 67(1)(b)

Repeal the paragraph, substitute:

(b) interception warrant information.

110 Paragraph 67(2)(a)

Omit "lawfully obtained information", substitute "lawfully intercepted information".

111 Paragraph 67(2)(b)

Repeal the paragraph, substitute:

(b) interception warrant information.

112 Section 68

Omit "lawfully obtained information", substitute "lawfully intercepted information".

113 Section 68

Omit "designated warrant information", substitute "interception warrant information".

Note: The heading to section 70 is altered by omitting "**Part V**" and substituting "**Part 2-3**".

114 Subsection 74(1)

Omit "lawfully obtained information", substitute "lawfully intercepted information".

115 Subsections 74(3), 76(2) and 76A(2)

Omit "designated warrant information", substitute "interception warrant information".

116 Subsection 77(3)

Omit "Designated warrant information", substitute "Interception warrant information".

Note: The heading to section 77 is altered by omitting "**designated warrant information**" and substituting "**interception warrant information**".

117 Subsections 77(3) and (4)

Omit "designated warrant information", substitute "interception warrant information".

118 Part VIII (heading)

Repeal the heading, substitute:

Part 2-7—Keeping and inspection of interception records of Commonwealth agencies

119 Paragraph 80(1)(b)

Omit "Part VI", substitute "Part 2-5".

120 Paragraph 80(1)(d)

Omit "Part VI warrant", substitute "Part 2-5 warrant".

121 Paragraph 81(1)(a)

Omit "Part VI warrant", substitute "Part 2-5 warrant".

122 Paragraph 81(1)(b)

Omit "Part VI", substitute "Part 2-5".

123 Paragraph 81(1)(c)

Omit "Part VI warrant", substitute "Part 2-5 warrant".

124 Paragraphs 81(1)(f), (g) and (h)

Omit "lawfully obtained information", substitute "lawfully intercepted information".

125 Paragraphs 81(2)(a), (b) and (ba)

Omit "Part VI warrant", substitute "Part 2-5 warrant".

126 Paragraphs 81(2)(d), (e) and (f)

Omit "lawfully obtained information", substitute "lawfully intercepted information".

127 Subsection 81(2A)

Omit "Part VI warrant", substitute "Part 2-5 warrant".

128 Subsection 81A(2)

Omit "Part VI warrant", substitute "Part 2-5 warrant".

129 Paragraphs 81C(3)(a) and (4)(a)

Omit "Part VI warrant", substitute "Part 2-5 warrant".

130 Subsection 84(1A) (note)

Omit "designated warrant information", substitute "interception warrant information".

131 Paragraph 92(3)(b)

Omit "lawfully obtained information", substitute "lawfully intercepted information".

132 Part IX (heading)

Repeal the heading, substitute:

Part 2-8—Reports about interceptions under Parts 2-3 and 2-5

Note 1: The heading to section 93 is altered by omitting "**Part V**" and substituting "**Part 2-3**".

Note 2: The heading to section 94 is altered by omitting "**Part VI**" and substituting "**Part 2-5**".

133 Paragraphs 94A(1)(a) and (b) and (3)(d)

Omit "Part VI", substitute "Part 2-5".

Note 1: The heading to section 97 is altered by omitting "**Part VI**" and substituting "**Part 2-5**".

Note 2: The heading to section 99 is altered by omitting "**Part VI**" and substituting "**Part 2-5**".

134 Subsections 100(1) and (2) and 101(1) and (2)

Omit "Part VI warrants" (wherever occurring), substitute "Part 2-5 warrants".

135 Subparagraph 102(1)(a)(ii)

Omit "lawfully obtained information", substitute "lawfully intercepted information".

136 Paragraph 102(1)(b)

Omit "lawfully obtained information", substitute "lawfully intercepted information".

137 Subparagraph 102(2)(a)(ii)

Omit "lawfully obtained information", substitute "lawfully intercepted information".

138 Paragraph 102(2)(b)

Omit "lawfully obtained information", substitute "lawfully intercepted information".

139 Paragraph 103(ab)

Omit "Part VI", substitute "Part 2-5".

140 Subsection 104(3)

Omit "Part V, or Parts VI, VII and VIII", substitute "Part 2-3, or Parts 2-5, 2-6 and 2-7".

141 Part X (heading)

Repeal the heading, substitute:

Part 2-9—Offences

142 Paragraphs 107(2)(a) and (b)

Omit "Part VIII", substitute "Part 2-7".

Note: The heading to section 107 is altered by omitting "**Part VIII**" and substituting "**Part 2-7**".

143 Part XA (heading)

Repeal the heading, substitute:

Part 2-10—Civil remedies

144 Part XI (heading)

Repeal the heading, substitute:

Chapter 5—Regulations

Part 5-1—Regulations

145 Section 108

Renumber as section 300.

Schedule 2—B-party interception

Telecommunications (Interception) Act 1979

1 After subparagraph 9(1)(a)(i)

Insert:

(ia) the means by which a person receives or sends a communication from or to another person who is engaged in, or reasonably suspected by the Director-General of Security of being engaged in, or of being likely to engage in, such activities; or

2 At the end of subsection 9(1)

Add:

Note: Subparagraph (a)(ia)—subsection (3) restricts the issuing of warrants if subparagraph (a)(ia) applies.

3 At the end of section 9

Add:

(3) The Attorney-General must not issue a warrant in a case in which subparagraph (1)(a)(ia) applies unless he or she is satisfied that:

(a) the Organisation has exhausted all other practicable methods of identifying the telecommunications services used, or likely to be used, by the other person referred to in subparagraph (1)(a)(ia); or

(b) interception of communications made to or from a telecommunications service used or likely to be used by that person would not otherwise be possible.

4 Subsection 9B(3)

Omit "period must not exceed 6 months, and the".

5 After subsection 9B(3)

Insert:

(3A) The specified period must not exceed:

(a) if subparagraph 9(1)(a)(ia) applies—3 months; or

(b) otherwise—6 months.

6 At the end of paragraphs 46(1)(a), (b) and (c)

Add "and".

7 Paragraph 46(1)(d)

Omit "which the person is involved; and", substitute:

which:

(i) the particular person is involved; or

(ii) another person is involved with whom the particular person is likely to communicate using the service; and

8 At the end of subsection 46(1)

Add:

Note: Subparagraph (d)(ii)—subsection (3) restricts the issuing of warrants if subparagraph (d)(ii) applies.

9 At the end of section 46

Add:

(3) The Judge or nominated AAT member must not issue a warrant in a case in which subparagraph (1)(d)(ii) applies unless he or she is satisfied that:

(a) the agency has exhausted all other practicable methods of identifying the telecommunications services used, or likely to be used, by the person involved in the offence or offences referred to in paragraph (1)(d); or

(b) interception of communications made to or from a telecommunications service used or likely to be used by that person would not otherwise be possible.

10 Subsection 49(3)

Omit "a period of up to 90 days", substitute:

a period of:

(a) if subparagraph 46(1)(d)(ii) applies—up to 45 days; or

(b) otherwise—up to 90 days.

11 After paragraph 100(1)(ec)

Insert:

(ed) in relation to applications of a kind referred to in paragraph (a), (b), (c), (d) or (e), the relevant statistics about applications of that kind that relate to warrants in relation to which subparagraph 46(1)(d)(ii) would apply if the warrants were issued; and

(ee) how many Part 2-5 warrants issued during that year on application made by the agency or authority were warrants in relation to which subparagraph 46(1)(d)(ii) applied; and

(ef) how many Part 2-5 warrants renewed during that year on application made by the agency or authority were warrants in relation to which subparagraph 46(1)(d)(ii) applied; and

12 After paragraph 100(2)(ec)

Insert:

(ed) in relation to applications of a kind referred to in paragraph (a), (b), (c), (d) or (e), the relevant statistics about applications of that kind that relate to warrants in relation to which subparagraph 46(1)(d)(ii) would apply if the warrants were issued; and

(ee) how many Part 2-5 warrants issued during that year were warrants in relation to which subparagraph 46(1)(d)(ii) applied; and

(ef) how many Part 2-5 warrants renewed during that year were warrants in relation to which subparagraph 46(1)(d)(ii) applied; and

13 At the end of paragraphs 101(1)(a), (b) and (c)

Add "and".

14 After paragraph 101(1)(d)

Insert:

(da) in relation to periods of a kind referred to in paragraph (a), (b), (c) or (d), the averages of the periods of that kind that relate to warrants in relation to which subparagraph 46(1)(d)(ii) applied; and

15 At the end of paragraphs 101(2)(a), (b) and (c)

Add "and".

16 After paragraph 101(2)(d)

Insert:

(da) in relation to periods of a kind referred to in paragraph (a), (b), (c) or (d), the averages of the periods of that kind that relate to warrants in relation to which subparagraph 46(1)(d)(ii) applied; and

Schedule 3—Equipment-based interception

Telecommunications (Interception) Act 1979

1 Subsection 5(1) (definition of *equipment*)

After "network,", insert "and includes a telecommunications device".

2 Subsection 5(1)

Insert:

telecommunications device means a terminal device that is capable of being used for transmitting or receiving a communication over a telecommunications system.

3 Subsection 5(1)

Insert:

telecommunications number means the address used by a carrier for the purposes of directing a communication to its intended destination and identifying the origin of the communication, and includes:

(a) a telephone number; and

(b) a mobile telephone number; and

(c) a unique identifier for a telecommunications device (for example, an electronic serial number or a Media Access Control address); and

(d) a user account identifier; and

(e) an Internet Protocol address; and

(f) an email address.

4 At the end of Part IA

Add:

6Q Identification of telecommunications device

For the purposes of this Act, a telecommunications device may be identified by:

(a) a unique telecommunications number assigned to it from time to time; or

(b) any other unique identifying factor.

5 Subsection 9A(1)

Repeal the subsection, substitute:

(1) Upon receiving a request by the Director-General of Security for the issue of a warrant under this section in respect of a person, the Attorney-General may, under his or her hand, issue a warrant in respect of the person if the Attorney-General is satisfied that:

(a) the person is engaged in, or reasonably suspected by the Director-General of Security of being engaged in, or of being likely to engage in, activities prejudicial to security; and

(b) the interception by the Organisation of:

(i) communications made to or from telecommunications services used by the person; or

(ii) communications made by means of a particular telecommunications device used by the person;

will, or is likely to, assist the Organisation in carrying out its function of obtaining intelligence relating to security; and

(c) relying on a telecommunications service warrant to obtain the intelligence would be ineffective.

(1A) The warrant authorises persons approved under section 12 in respect of the warrant to intercept, subject to any conditions or restrictions that are specified in the warrant:

(a) communications that are being made to or from any telecommunications service that the person is using, or is likely to use; or

(b) communications that are being made by means of a telecommunications device, identified in the warrant, that the person is using, or is likely to use.

Note: Subsection (3) restricts the issuing of a warrant authorising interception of communications made by means of a telecommunications device identified in the warrant.

(1B) The warrant may authorise entry on any premises specified in the warrant for the purpose of installing, maintaining, using or recovering any equipment used to intercept such communications.

6 Saving provision

The repeal and substitution of subsection 9A(1) of the *Telecommunications (Interception) Act 1979* by this Schedule does not affect the validity of a warrant issued under that subsection before the commencement of this Schedule.

7 After paragraph 9A(2)(b)

Insert:

(ba) if the warrant would authorise interception of communications made by means of a telecommunications device identified in the warrant—must include details sufficient to identify the telecommunications device that the person is using, or is likely to use; and

8 At the end of section 9A

Add:

(3) The Attorney-General must not issue a warrant that authorises interception of communications made by means of a telecommunications device identified in the warrant unless he or she is satisfied that:

(a) there are no other practicable methods available to the Organisation at the time of making the application to identify the telecommunications services used, or likely to be used, by the person in respect of whom the warrant would be issued; or

(b) interception of communications made to or from a telecommunications service used, or likely to be used, by that person would not otherwise be practicable.

9 Subsection 11B(1)

Repeal the subsection, substitute:

(1) The Attorney-General may, under his or her hand, issue a warrant in respect of a person if:

(a) the Director-General of Security gives a notice in writing to the Attorney-General requesting the Attorney-General to issue a warrant under this section authorising persons approved under section 12 in respect of the warrant to do acts or things referred to in subsection 9A(1A) in relation to:

(i) communications that are being made to or from any telecommunications service that a person or foreign organisation is using, or is likely to use; or

(ii) communications that are being made by means of a particular telecommunications device that a person or foreign organisation is using, or is likely to use;

for the purpose of obtaining foreign intelligence relating to a matter specified in the notice; and

(b) the Attorney-General is satisfied, on the basis of advice received from the relevant Minister, that:

(i) the obtaining of foreign intelligence relating to that matter is important in relation to the defence of the Commonwealth or to the conduct of the Commonwealth's international affairs; and

(ii) it is necessary to intercept the communications of the person or foreign organisation in order to obtain the intelligence referred to in paragraph (a); and

(iii) relying on a telecommunications service warrant to obtain the intelligence would be ineffective.

(1A) The warrant authorises persons approved under section 12 in respect of the warrant to intercept, subject to any conditions or restrictions that are specified in the warrant:

(a) communications that are being made to or from any telecommunications service that the person or foreign organisation is using, or is likely to use; or

(b) communications that are being made by means of a telecommunications device, identified in the warrant, that the person or foreign organisation is using, or is likely to use.

Note: Subsection (3) restricts the issuing of a warrant authorising interception of communications made by means of a telecommunications device identified in the warrant.

(1B) The warrant may authorise entry on any premises specified in the warrant for the purpose of installing, maintaining, using or recovering any equipment used to intercept such communications.

10 Saving provision

The repeal and substitution of subsection 11B(1) of the *Telecommunications (Interception) Act 1979* by this Schedule does not affect the validity of a warrant issued under that subsection before the commencement of this Schedule.

11 After paragraph 11B(2)(b)

Insert:

(ba) if the warrant would authorise interception of communications made by means of a telecommunications device identified in the warrant—must include details sufficient to identify the telecommunications device that the person or foreign organisation is using, or is likely to use; and

12 At the end of section 11B (before the note)

Add:

(3) The Attorney-General must not issue a warrant that authorises interception of communications made by means of a telecommunications device identified in the warrant unless he or she is satisfied that:

(a) there are no other practicable methods available to the Organisation at the time of making the application to identify the telecommunications services used, or likely to be used, by the person or foreign organisation in respect of whom or which the warrant would be issued; or

(b) interception of communications made to or from a telecommunications service used, or likely to be used, by that person or foreign organisation would not otherwise be practicable.

13 After paragraph 16(1)(a)

Insert:

(aa) the warrant is not a warrant that authorises interception of communications made by means of a telecommunications device identified in the warrant; and

14 After subsection 16(1)

Insert:

(1A) Where:

(a) the Managing Director of a carrier has been given a copy of a warrant under section 9A or 11B; and

(b) the warrant is a warrant that authorises interception of communications made by means of a telecommunications device identified in the warrant; and

(c) it is proposed, under the warrant, to intercept, by means of a telecommunications device, communications made to or from a telecommunications service operated by the carrier; and

(d) the device was not identified in the warrant;

a certifying person must cause the Managing Director of the carrier to be given, as soon as practicable, a description in writing of the device sufficient to identify it.

15 Paragraph 16(2)(a)

After "from which", insert ", or a telecommunications device by means of which,".

16 Paragraph 16(2)(b)

After "that service", insert ", or by means of that device,".

17 After paragraph 42(4A)(b)

Insert:

(ba) if the warrant would authorise interception of communications made by means of a telecommunications device identified in the warrant—details sufficient to identify the telecommunications device that the person is using, or is likely to use; and

18 Paragraph 46A(1)(d)

Repeal the paragraph, substitute:

(d) information that would be likely to be obtained by intercepting under a warrant:

(i) communications made to or from any telecommunications service that the person is using, or is likely to use; or

(ii) communications made by means of a particular telecommunications device that a person is using, or is likely to use;

would be likely to assist in connection with the investigation by the agency of a class 2 offence, or class 2 offences, in which the person is involved; and

19 At the end of subsection 46A(1)

Add:

Note: Subsection (3) restricts the issuing of a warrant authorising interception of communications made by means of a telecommunications device identified in the warrant.

20 Paragraph 46A(2)(a)

Repeal the paragraph, substitute:

(a) how much the privacy of any person or persons would be likely to be interfered with by intercepting under a warrant:

(i) communications made to or from any telecommunications service used, or likely to be used, by the person in respect of whom the warrant is sought; or

(ii) communications made by means of a particular telecommunications device used, or likely to be used, by the person in respect of whom the warrant is sought;

as the case requires; and

21 At the end of section 46A

Add:

(3) The Judge or nominated AAT member must not issue a warrant that authorises interception of communications made by means of a telecommunications device identified in the warrant unless he or she is satisfied that:

(a) there are no other practicable methods available to the agency at the time of making the application to identify the telecommunications services used, or likely to be used, by the person in respect of whom the warrant would be issued; or

(b) interception of communications made to or from a telecommunications service used, or likely to be used, by that person would not otherwise be practicable.

22 After paragraph 60(4)(a)

Insert:

(aa) the warrant is not a warrant that authorises interception of communications made by means of a telecommunications device identified in the warrant; and

23 After subsection 60(4)

Insert:

(4A) Where:

(a) the Managing Director of a carrier has been informed, under subsection (1), of the issue of a named person warrant; and

(b) the warrant is a warrant that authorises interception of communications made by means of a telecommunications device identified in the warrant; and

(c) it is proposed, under the warrant, to intercept, by means of a telecommunications device, communications made to or from a telecommunications service operated by the carrier; and

(d) the device was not identified in the warrant;

a certifying person must cause the Managing Director of the carrier to be given, as soon as practicable, a description in writing of the device sufficient to identify it.

24 Paragraph 60(5)(b)

After "particular service", insert ", or by means of a particular device,".

Schedule 4—Class 1 and class 2 offences

Part 1—Amendments

Telecommunications (Interception) Act 1979

1 Subsection 5(1) (definition of *class 1 offence*)

Repeal the definition.

2 Subsection 5(1) (definition of *class 2 offence*)

Repeal the definition.

3 Subsection 5(1) (definition of *named person warrant*)

Omit ", 45A".

4 Subsection 5(1) (paragraph (a) of the definition of *prescribed offence*)

Repeal the paragraph, substitute:

(a) a serious offence, or an offence that was a serious offence when the offence was committed;

5 Subsection 5(1) (definition of *serious offence*)

Repeal the definition, substitute:

serious offence has the meaning given by section 5D.

6 Subsection 5(1) (definition of *telecommunications service warrant*)

Omit "45,".

7 Subsection 5D(1)

Repeal the subsection, substitute:

General types of serious offences

(1) An offence is a ***serious offence*** if it is:

(a) a murder, or an offence of a kind equivalent to murder; or

(b) a kidnapping, or an offence of a kind equivalent to kidnapping; or

(c) an offence against Division 307 of the *Criminal Code*; or

(d) an offence constituted by conduct involving an act or acts of terrorism; or

(e) an offence against Division 72, 101, 102 or 103 of the *Criminal Code*; or

(f) except for the purposes of an application for a warrant by an agency other than the ACC, an offence in relation to which the ACC is conducting a special investigation.

Note: The heading to section 5D is replaced by the heading "**Serious offences**".

8 Subsection 5D(2)

Omit "is a ***class 2 offence***", substitute "is also a ***serious offence***".

Note: The heading to subsection 5D(2) is deleted.

9 Subsections 5D(2A), (3), (3A), (4), (5) and (5A)

Omit "***class 2 offence***", substitute "***serious offence***".

Note: The following heading to subsection 5D(2A) is inserted "*Telecommunications offences*".

10 Subsection 5D(5A)

Omit "Division 307 or".

11 Subsection 5D(6)

Omit "***class 2 offence***", substitute "***serious offence***".

Note: The heading to subsection 5D(6) is altered by omitting "*class 2 offences*" and substituting "*serious offences*".

12 Subsection 5D(6)

Omit "class 2 offence", substitute "serious offence".

13 At the end of section 5D

Add:

(7) An offence is also a ***serious offence*** if it is an offence constituted by receiving or assisting a person who is, to the offender's knowledge, guilty of a serious offence mentioned in subsection (1),

in order to enable the person to escape punishment or to dispose of the proceeds of the offence.

14 Paragraph 6H(a)

Repeal the paragraph, substitute:

(a) in the case of a warrant under section 48—paragraphs 46(1)(c) and (d); or

15 Paragraph 6H(b)

Omit "45(c) and (d), 45A (c) and (d),".

16 Subsection 7(9)

Repeal the subsection, substitute:

(9) The doing of an act mentioned in subparagraph (4)(b)(ii) or (iii) or (5)(b)(ii) or (iii) in a particular case is taken to constitute a serious offence, even if it would not constitute a serious offence apart from this subsection.

Note: See subsection (6). A Part 2-5 warrant can only be issued for the purposes of an investigation relating to the commission of a serious offence.

17 Sections 45 and 45A

Repeal the sections.

18 Paragraphs 46(1)(d) and 46A(1)(d)

Omit "a class 2 offence, or class 2 offences,", substitute "a serious offence, or serious offences,".

Note: The headings to sections 46 and 46A are altered by omitting "**in relation to class 2 offence**".

19 Section 47

Omit "45, 45A,".

20 Subsection 48(1)

Omit "45 or" (wherever occurring).

21 Paragraph 48(3)(c)

Omit "45 or".

22 Subparagraph 48(3)(d)(ii)

Omit "45 or".

23 Paragraph 49(7)(a)

Repeal the paragraph, substitute:

(a) in the case of a warrant under section 48—paragraph 46(1)(d); or

24 Paragraph 49(7)(b)

Omit "45(d), 45A(d),".

25 Subsection 54(1)

Omit "45, 45A,".

26 Subsection 61(3)

Omit "45, 45A,".

27 Subparagraph 81A(2)(g)(i)

Repeal the subparagraph, substitute:

(i) in the case of a warrant under section 48—paragraph 46(1)(d); or

28 Subparagraph 81A(2)(g)(ii)

Omit "45(d), 45A(d),".

29 Subparagraph 81C(2)(g)(i)

Repeal the subparagraph, substitute:

(i) in the case of a warrant under section 48—paragraph 46(1)(d); or

30 Subparagraph 81C(2)(g)(ii)

Omit "45(d), 45A(d),".

Part 2—Transitional provisions

31 Pending applications

(1) The *Telecommunications (Interception) Act 1979* as amended by this Schedule applies to applications made before the commencement of this Schedule for warrants under section 45 of that Act that:

(a) were made before the commencement of this Schedule; and

(b) were not refused or withdrawn before that commencement;

as if they were applications made for warrants under section 46 of that Act.

(2) The *Telecommunications (Interception) Act 1979* as amended by this Schedule applies to applications made before the commencement of this Schedule for warrants under section 45A of that Act that:

(a) were made before the commencement of this Schedule; and

(b) were not refused or withdrawn before that commencement;

as if they were applications made for warrants under section 46A of that Act.

32 Continuation of warrants under sections 45 and 45A

(1) A warrant that was issued before the commencement of this Schedule under section 45 of the *Telecommunications (Interception) Act 1979* and that was in force immediately before that commencement continues in force after that commencement as if it had been issued under section 46 of that Act.

(2) A warrant that was issued before the commencement of this Schedule under section 45A of the *Telecommunications (Interception) Act 1979* and that was in force immediately before that commencement continues in force after that commencement as if it had been issued under section 46A of that Act.

33 Warrants under sections 46, 46A and 48 unaffected

The amendments of sections 46, 46A and 48 of the *Telecommunications (Interception) Act 1979* made by this Schedule do not affect the validity of warrants issued under those sections before the commencement of this Schedule.

34 Renewals of warrants

To avoid doubt, a warrant issued after the commencement of this Schedule under section 46 or 46A of the *Telecommunications (Interception) Act 1979* may be, for the purposes of that Act, a renewal of a warrant issued before that commencement under section 45 or 45A of that Act.

Schedule 5—Transfer of functions

Telecommunications (Interception) Act 1979

1 Subsection 5(1) (subparagraph (a)(v) of the definition of *permitted purpose*)

Omit "the Chief Executive Officer of the ACC by subsections 80(2), 81(2) and 81(3)", substitute "the chief officer of a Commonwealth agency by sections 80 and 81".

2 Division 1 of Part VI

Repeal the Division.

3 Paragraph 35(1)(a)

Omit "subsections 80(2) and 81(2) and (3) impose on the Chief Executive Officer of the ACC", substitute "sections 80 and 81 impose on the chief officer of a Commonwealth agency".

4 Section 47

Repeal the section, substitute:

47 Limit on authority conferred by warrant

A warrant issued under section 46 or 46A does not authorise the interception of communications passing over a telecommunications system that a carrier operates unless:

(a) notification of the issue of the warrant has been received by or on behalf of the Managing Director of the carrier under subsection 60(1); and

(b) the interception takes place as a result of action taken by an employee of the carrier.

5 Subsection 52(2)

Omit "other than the Australian Federal Police".

6 Paragraphs 52(2)(a) and (b)

Omit "Commissioner of Police", substitute "Secretary of the Department".

7 Subsection 53(1)

Omit "other than the Australian Federal Police".

Note: The heading to section 53 is replaced by the heading "**Notification of issue of warrants**".

8 Paragraphs 53(1)(a), (b) and (c)

Omit "Commissioner of Police", substitute "Secretary of the Department".

9 Section 54

Repeal the section, substitute:

54 Entry into force of warrants

A warrant comes into force when it is issued.

10 Section 56

Repeal the section.

11 Subsections 57(1) and (2)

Repeal the subsections, substitute:

(1) The chief officer of an agency must, on being satisfied that the grounds on which a warrant was issued to the agency have ceased to exist:

(a) cause the Secretary of the Department to be informed forthwith that the chief officer proposes to revoke the warrant; and

(b) cause the chief officer of any other agency that is exercising authority under the warrant to be informed forthwith of the proposed revocation of the warrant; and

(c) by writing signed by him or her, revoke the warrant.

(2) The chief officer of an agency may at any time, by writing signed by him or her, revoke a warrant issued to the agency after:

(a) causing the Secretary of the Department to be informed of the proposed revocation; and

(b) causing the chief officer of any other agency that is exercising authority under the warrant to be informed

forthwith that the chief officer proposes to revoke the warrant.

Note: The heading to section 57 is altered by omitting "**of other agency**".

12 Paragraphs 57(3)(a) and (b)

Omit "Commissioner of Police", substitute "Secretary of the Department".

13 At the end of section 57

Add:

(5) This section does not apply in relation to a warrant that has ceased to be in force.

14 Subsection 58(1)

Repeal the subsection, substitute:

(1) The chief officer of an agency must, on the revocation or proposed revocation of a warrant issued to the agency, forthwith take such steps as are necessary to ensure that interceptions of communications under the warrant are discontinued.

15 Subsection 58(2)

Omit "subsection 56(2) or".

16 Section 59

Omit "Commissioner of Police", substitute "Secretary of the Department".

17 Paragraph 60(2)(a)

Omit "Commissioner of Police", substitute "Secretary of the Department".

18 Subsection 61(3)

Repeal the subsection.

19 Saving provision

A certificate issued under subsection 61(3) of the *Telecommunications (Interception) Act 1979* that had effect immediately before the repeal of that subsection by this Act has effect after that repeal as if that subsection had not been repealed.

20 Subsection 61(5)

Omit "(3) or".

21 Subsection 79(2)

Omit "Commissioner of Police", substitute "Secretary of the Department".

22 Part 2-7 (heading)

Repeal the heading, substitute:

Part 2-7—Keeping and inspection of interception records

23 Sections 80 and 81

Repeal the sections, substitute:

80 Commonwealth agencies to keep documents connected with issue of warrants

The chief officer of a Commonwealth agency must cause to be kept in the agency's records:

(a) each warrant issued to the agency; and

(b) a copy of each notification under paragraph 53(1)(b) of the issue of such a warrant, being a notification given to the Secretary of the Department; and

(c) each instrument revoking such a warrant; and

(d) a copy of each certificate issued under subsection 61(4) by a certifying officer of the agency; and

(e) each authorisation by the chief officer under subsection 66(2).

81 Other records to be kept by Commonwealth agencies in connection with interceptions

(1) The chief officer of a Commonwealth agency must cause:

(a) particulars of each telephone application for a Part 2-5 warrant made by the agency; and

(b) in relation to each application by the agency for a Part 2-5 warrant, a statement as to whether:

(i) the application was withdrawn or refused; or

(ii) a warrant was issued on the application; and

(c) in relation to each Part 2-5 warrant whose authority is exercised by the agency, particulars of:

(i) the warrant; and

(ii) the day on which, and the time at which, each interception under the warrant began; and

(iii) the duration of each such interception; and

(iv) the name of the person who carried out each such interception; and

(v) in relation to a named person warrant—each service to or from which communications have been intercepted under the warrant; and

(d) in relation to each restricted record that has at any time been in the agency's possession, particulars of:

(i) if the restricted record is a record obtained by an interception under a warrant issued to the agency—that warrant; and

(ii) each occasion when the restricted record came (whether by its making or otherwise) to be in the agency's possession; and

(iii) each occasion (if any) when the restricted record ceased (whether by its destruction or otherwise) to be in the agency's possession; and

(iv) each other agency or other body (if any) from or to which, or other person (if any) from or to whom, the agency received or supplied the restricted record; and

(e) particulars of each use made by the agency of lawfully intercepted information; and

(f) particulars of each communication of lawfully intercepted information by an officer of the agency to a person or body other than such an officer; and

(g) particulars of each occasion when, to the knowledge of an officer of the agency, lawfully intercepted information was given in evidence in a relevant proceeding in relation to the agency;

to be recorded in writing or by means of a computer as soon as practicable after the happening of the events to which the particulars relate or the statement relates, as the case may be.

(2) If a Part 2-5 warrant is a named person warrant, the particulars referred to in subparagraph (1)(c)(ii) must indicate the service in respect of which each interception occurred.

(3) The chief officer of a Commonwealth agency must cause to be kept in the agency's records each record that the chief officer has caused to be made under this section.

24 Subsections 81A(1) and (2)

Omit "Commissioner of Police", substitute "Secretary of the Department".

25 Saving provision

The General Register of Warrants kept by the Commissioner of Police before the commencement of this item is taken, after that commencement, to be the General Register of Warrants kept by the Secretary of the Department.

26 Subsection 81B(1)

Repeal the subsection, substitute:

(1) Within 3 months after the commencement of Schedule 5 to the *Telecommunications (Interception) Amendment Act 2006*, the Secretary of the Department must deliver the General Register to the Minister for inspection.

27 Subsection 81B(2)

Omit "Commissioner of Police", substitute "Secretary of the Department".

28 Subsections 81C(1) and (2)

Omit "Commissioner of Police", substitute "Secretary of the Department".

29 Saving provision

The Special Register of Warrants kept by the Commissioner of Police before the commencement of this item is taken, after that commencement, to be the Special Register of Warrants kept by the Secretary of the Department.

30 Subsection 81D(1)

Repeal the subsection, substitute:

Original submission

(1) Within 3 months after the commencement of Schedule 5 to the *Telecommunications (Interception) Amendment Act 2006*, the Secretary of the Department must deliver the Special Register to the Minister for inspection by the Minister.

31 Subsections 81D(2) and (3)

Omit "Commissioner of Police", substitute "Secretary of the Department".

32 Subsection 81E(2)

Omit "Commissioner of Police" (first occurring), substitute "Secretary of the Department".

Note: The heading to subsection 81E(2) is altered by omitting "*Commissioner*" and substituting "*Secretary*".

33 Subsection 81E(2)

Omit "Commissioner of Police" (second and third occurring), substitute "Secretary".

34 Saving provision

A notice given under section 81E of the *Telecommunications (Interception) Act 1979* that had effect immediately before the commencement of this Schedule has effect after that commencement as if it were a notice by the Secretary requiring the information concerned to be given to the Secretary.

35 Section 82

Repeal the section.

36 At the end of paragraph 86(1)(a)

Add "and".

37 After paragraph 86(1)(b)

Insert:

and (ba) is entitled to have full and free access at all reasonable times to the General Register and the Special Register; and

38 Paragraph 86(1)(c)

After "agency", insert "or the General Register or Special Register".

39 At the end of section 86

Add:

(3) The Ombudsman's powers include doing anything incidental or conducive to the performance of any of the Ombudsman's functions under this Part.

Schedule 6—Other amendments

Telecommunications (Interception) Act 1979

1 Subsection 5(1) (subparagraph (f)(ii) of the definition of *permitted purpose*)

Repeal the subparagraph, substitute:

(ii) an investigation by the Director, Police Integrity under the Police Regulation Act or the Whistleblowers Protection Act, into serious misconduct (within the meaning of the Police Regulation Act); or

2 Subsection 5(1) (at the end of paragraphs (a), (b) and (c) of the definition of *prescribed offence*)

Add "or".

3 Subsection 5(1)

Insert:

Whistleblowers Protection Act means the *Whistleblowers Protection Act 2001* of Victoria.

4 Paragraph 5D(4)(b)

Repeal the paragraph, substitute:

(b) Division 1A of Part IV of the *Crimes Act 1900* of New South Wales;

5 Subsection 6(2)

Repeal the subsection.

6 Subsection 7(11)

Repeal the subsection.

7 Subsection 12(1)

Omit "(1)".

8 Subsection 55(5)

After "designated officer", insert ", or an employee of a carrier,".

9 Section 78

Omit "in Part IIA or".

10 Paragraphs 81C(3)(a) and (4)(a)

After "warrant", insert "has been issued".

[*Minister's second reading speech made in—*
House of Representatives on 16 February 2006
Senate on 1 March 2006]

(10/06)