Cybercrime Legislation AmendmentAct 2012

No. 120, 2012

An Act to implement the Council of Europe Convention on Cybercrime, and for other purposes

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

Contents

1 Short title 1
2 Commencement 2
3 Schedule(s) 3

Schedule 1—Preservation regime for stored communications 4

Telecommunications Act 1997 4

Telecommunications (Interception and Access) Act 1979 4

Schedule 2—Amendments relating to Mutual Assistance 22

Part 1—Stored communications 22

Mutual Assistance in Criminal Matters Act 1987 22

Telecommunications (Interception and Access) Act 1979 23

Part 2—Telecommunications data 28

Mutual Assistance in Criminal Matters Act 1987 28

Telecommunications Act 1997 29

Telecommunications (Interception and Access) Act 1979 29

Part 3—Recovery of costs by carriage service providers etc. for providing assistance to Australian law enforcement authorities 40

Telecommunications Act 1997 40

Schedule 3—Computer offences amendments 41

Criminal Code Act 1995 41

Schedule 4—Telecommunications data confidentiality 43

Telecommunications (Interception and Access) Act 1979 43

Schedule 5—Miscellaneous 48

Telecommunications (Interception and Access) Act 1979 48

Cybercrime Legislation AmendmentAct 2012

No. 120, 2012

An Act to implement the Council of Europe Convention on Cybercrime, and for other purposes

[*Assented to 12 September 2012*]

The Parliament of Australia enacts:

1 Short title

This Act may be cited as the *Cybercrime Legislation Amendment Act 2012*.

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	Column 2	Column 3
Provision(s)	**Commencement**	**Date/Details**
1. Sections 1 to 3 and anything in this Act not elsewhere covered by this table	The day this Act receives the Royal Assent.	12 September 2012
2. Schedules 1 and 2	The 28th day after this Act receives the Royal Assent.	
3. Schedule 3	The later of: (a) the day this Act receives the Royal Assent; and (b) the day the Council of Europe Convention on Cybercrime, done at Budapest on 23 November 2001, comes into force for Australia. However, the provision(s) do not commence at all if the event mentioned in paragraph (b) does not occur within the period of 6 months beginning on the day this Act receives the Royal Assent. The Minister must announce by notice in the *Gazette* the day the Council of Europe Convention on Cybercrime comes into force for Australia.	
4. Schedules 4 and 5	The 28th day after this Act receives the Royal Assent.	

Note: This table relates only to the provisions of this Act as originally enacted. It will not be amended to deal with any later amendments of this Act.

(2) Any information in column 3 of the table is not part of this Act. Information may be inserted in this column, or information in it may be 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—Preservation regime for stored communications

Telecommunications Act 1997

1 After paragraph 313(7)(c)

Insert:

(ca) complying with a domestic preservation notice or a foreign preservation notice that is in force under Part 3-1A of that Act; or

Telecommunications (Interception and Access) Act 1979

2 Subsection 5(1)

Insert:

certifying official, of an issuing agency, means:

(a) if the issuing agency is an enforcement agency(including an interception agency)—a certifying officer of the agency; and

(b) if the issuing agency is the Organisation—a certifying person of the Organisation.

3 Subsection 5(1)

Insert:

domestic preservation notice has the meaning given by subsection 107H(1).

4 Subsection 5(1)

Insert:

foreign preservation notice has the meaning given by subsection107N(1).

5 Subsection 5(1)

Insert:

historic domestic preservation notice has the meaning given by subparagraph 107H(1)(b)(i).

8 Subsection 5(1)

Insert:

issuing agency, in relation to a preservation notice, means the agency that gives the notice.

9 Subsection 5(1)

Insert:

ongoing domestic preservation notice has the meaning given by subparagraph 107H(1)(b)(ii).

10 Subsection 5(1)

Insert:

preservation notice means a domestic preservation notice or a foreign preservation notice.

11 Subsection 5(1)

Insert:

preservation notice information has the meaning given by section 6EAA.

12 Subsection 5(1)

Insert:

preserve, in relation to a stored communication, means maintain the integrity of:

(a) the stored communication; or

(b) a copy of the stored communication.

13 Subsection 5(1)

Insert:

relates:

(a) a stored communication ***relates*** to a person only if it is:

(i) a stored communication that the person has made; or

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

(b) a stored communication ***relates*** to a telecommunications service only if it has passed over a telecommunications system by way of the telecommunications service.

14 Subsection 5(1)

Insert:

relevant period, for a domestic preservation notice, means:

(a) for an historic domestic preservation notice—the period referred to in subparagraph 107H(1)(b)(i); and

(b) for an ongoing domestic preservation notice—the period referred to in subparagraph 107H(1)(b)(ii).

15 Subsection 5(1)

Insert:

working day means any day except:

(a) a Saturday or a Sunday; or

(b) a day that is a public holiday in any State or Territory.

16 After section 6EA

Insert:

6EAA Preservation notice information

A reference in this Act to ***preservation notice information*** is a reference to:

(a) information about any of the following:

(i) the giving of a preservation notice;

(ii) for a foreign preservation notice—the making of a request under section 107P to preserve stored communications covered by the notice;

(iii) the existence or non-existence of a preservation notice;

(iv) the expiry of a preservation notice; or

(b) any other information that is likely to enable the identification of:

(i) the person or telecommunications service specified in a preservation notice; or

(ii) the person or telecommunications service to which a preservation notice relates.

17 Chapter 3 (heading)

Repeal the heading, substitute:

Chapter 3—Preserving and accessing stored communications

18 Before Part 3-1

Insert in Chapter 3:

Part 3-1A—Preserving stored communications

Division 1—Outline of this Part

107G Outline of this Part

This Part establishes a system of preserving certain stored communications that are held by a carrier. The purpose of the preservation is to prevent the communications from being destroyed before they can be accessed under certain warrants issued under this Act.

Under the system, certain agencies can give a preservation notice to a carrier requiring the carrier to preserve all stored communications that the carrier holds that relate to the person or telecommunications service specified in the notice. The carrier will breach its obligations under section 313 of the *Telecommunications Act 1997* if it does not comply with the notice.

There are 2 types of preservation notices: domestic preservation notices (which cover stored communications that might relate either to a contravention of certain Australian laws or to security) and foreign preservation notices (which cover stored communications that might relate to a contravention of certain foreign laws).

Division 2 deals with domestic preservation notices. There are 2 kinds of domestic preservation notices:

(a) historic domestic preservation notices, which cover stored communications held by the carrier on a particular day; and

(b) ongoing domestic preservation notices, which cover stored communications held by the carrier in a particular 30-day period.

An issuing agency (which is an enforcement agency or the Organisation for an historic domestic preservation notice, and an interception agency or the Organisation for an ongoing domestic preservation notice) can only give a domestic preservation notice if the conditions in section 107J are satisfied. There are certain grounds on which the notice must be revoked (see section 107L).

Division 3 deals with foreign preservation notices. Foreign preservation notices, like historic domestic preservation notices, cover stored communications held by the carrier on a particular day. Only the Australian Federal Police can give a foreign preservation notice to a carrier and it can only do so if a foreign country has made a request for the preservation in accordance with section 107P. There are certain grounds on which the notice must be revoked (see section 107R).

Division 4 has miscellaneous provisions relating to both domestic and foreign preservation notices (such as provisions about the giving of evidentiary certificates by carriers and issuing agencies).

The Ombudsman has functions in relation to preservation notices given by issuing agencies (other than the Organisation) and the Inspector-General of Intelligence and Security has functions in relation to preservation notices given by the Organisation.

Division 2—Domestic preservation notices

107H Domestic preservation notices

(1) An issuing agency may give a carrier a written notice (a ***domestic preservation notice***) requiring the carrier to preserve, while the notice is in force, all stored communications that:

(a) relate to the person or telecommunications service specified in the notice; and

(b) the carrier holds at any time during:

(i) the period that starts at the time the carrier receives the notice and ends at the end of the day the carrier receives the notice (in which case the notice is an ***historic domestic preservation notice***); or

(ii) the period that starts at the time the carrier receives the notice and ends at the end of the 29th day after the day the carrier receives the notice (in which case the notice is an ***ongoing domestic preservation notice***).

(2) However, the agency can only give the notice if the conditions in subsection 107J(1) or (2) are satisfied.

(3) In the notice, the agency can only specify:

(a) one person; or

(b) one or more telecommunications services; or

(c) one person and one or more telecommunications services.

107J Conditions for giving domestic preservation notices

Notices given by enforcement agencies or interception agencies

(1) A domestic preservation notice may be given under subsection 107H(1) if:

(a) the issuing agency is:

(i) for an historic domestic preservation notice—an enforcement agency; and

(ii) for an ongoing domestic preservation notice—an enforcement agency that is aninterception agency; and

(b) the agency is investigating a serious contravention; and

(c) the agency considers that there are reasonable grounds for suspecting that, in the relevant period for the notice, there are stored communications in existence, or stored communications might come into existence, that:

(i) might assist in connection with the investigation; and

(ii) relate to the person or telecommunications service specified in the notice; and

(d) the agency intends that if, at a later time, the agency considers that the stored communications would be likely to assist in connection with the investigation, then the agency

will apply for a Part 2-5 warrant or a stored communications warrant to access those communications; and

(e) for an ongoing domestic preservation notice—there is not another ongoing domestic preservation notice in force that:

(i) was given by the agency to the same carrier; and

(ii) specifies the same person or telecommunications service.

Notices given by the Organisation

(2) A domestic preservation notice may be given under subsection 107H(1) if:

(a) the issuing agency is the Organisation; and

(b) the Organisation considers that there are reasonable grounds for suspecting that, in the relevant period for the notice, there are stored communications in existence, or stored communications might come into existence, that:

(i) might assist the Organisation in carrying out its function of obtaining intelligence relating to security; and

(ii) relate to the person or telecommunications service specified in the notice; and

(c) the Organisation intends that if, at a later time, the Organisation considers that the stored communications would be likely to assist in carrying out that function, then the Director-General of Security will request a Part 2-2 warrant to access those communications; and

(d) for an ongoing domestic preservation notice—there is not another ongoing domestic preservation notice in force that:

(i) was given by the Organisation to the same carrier; and

(ii) specifies the same person or telecommunications service.

107K When a domestic preservation notice is in force

A domestic preservation notice:

(a) comes into force when the carrier receives it; and

(b) ceases to be in force at the earliest of the following times:

(i) the end of the period of 90 days, starting on the day the carrier receives it;

(ii) if the notice is revoked under section 107L—when the carrier receives notice of the revocation;

(iii) if a Part 2-5 warrant or stored communications warrant authorising access to the stored communications covered by the notice is issued in relation to the issuing agency—when the warrant ceases to be in force;

(iv) if a Part 2-2 warrant authorising access to the stored communications covered by the notice is issued in relation to the issuing agency—the end of the period of 5 days after the day the warrant was issued.

107L Revoking a domestic preservation notice

Discretionary revocation

(1) An issuing agency that has given a domestic preservation notice may revoke the notice at any time.

Mandatory revocation

(2) An issuing agency that has given a domestic preservation notice must revoke the notice if:

(a) if the issuing agency is an enforcement agency (including an interception agency):

(i) the condition in paragraph 107J(1)(b) or (c) is no longer satisfied; or

(ii) the agency decides not to apply for a Part 2-5 warrant or stored communications warrant to access the stored communications covered by the notice; or

(b) if the issuing agency is the Organisation:

(i) the condition in paragraph 107J(2)(b) is no longer satisfied; or

(ii) the Organisation is satisfied that the Director-General of Security will not request a Part 2-2 warrant to access the stored communications covered by the notice.

Revocation effected by giving revocation notice

(3) A domestic preservation notice is revoked by the issuing agency giving the carrier to whom it was given written notice of the revocation.

107M Persons who act on the issuing agency's behalf

Historic domestic preservation notices

(1) An historic domestic preservation notice may only be given or revoked on behalf of an issuing agency by:
  (a) if the issuing agency is an enforcement agency—a person who may, under section 110, apply on the agency's behalf for a stored communications warrant to access the stored communications covered by the notice; and
  (b) if the issuing agency is the Organisation—a certifying person.

Ongoing domestic preservation notices

(2) An ongoing domestic preservation notice may only be given on behalf of an issuing agency by:
  (a) if the issuing agency is anenforcement agency that is an interception agency—an authorised officer of the agency; and
  (b) if the issuing agency is the Organisation—the Director-General of Security.

(3) An ongoing domestic preservation notice may only be revoked on behalf of an issuing agency by:
  (a) if the issuing agency is anenforcement agency that is an interception agency—an authorised officer of the agency; and
  (b) if the issuing agency is the Organisation—a certifying person.

Division 3—Foreign preservation notices

107N When a foreign preservation notice can be given

(1) If the Australian Federal Police receives a request in accordance with section 107P, the Australian Federal Police must give the carrier to which the request relates a written notice (a ***foreign preservation notice***) requiring the carrier to preserve, while the notice is in force, all stored communications that:
  (a) relate to the person or telecommunications service specified in the notice; and

(b) the carrier holds at any time during the period that starts at the time the carrier receives the notice and ends at the end of the day the carrier receives the notice.

(2) In the notice, the Australian Federal Police can only specify:
(a) one person; or
(b) one or more telecommunications services; or
(c) one person and one or more telecommunications services.

107P Condition for giving a foreign preservation notice

(1) If, under paragraph 15B(d) of the *Mutual Assistance in Criminal Matters Act 1987*, a foreign country intends to request the Attorney-General to arrange for access to stored communications that:
(a) relate to a specified person or specified telecommunications service; and
(b) are held by a carrier; and
(c) are relevant to an investigation, or investigative proceeding, relating to a criminal matter involving a serious foreign contravention;
then the foreign country may request the Australian Federal Police to arrange for the preservation of those stored communications.

(2) The request to the Australian Federal Police must:
(a) be in writing; and
(b) specify the name of the authority concerned with the criminal matter; and
(c) specify the serious foreign contravention that is the subject of the investigation or investigative proceeding; and
(d) specify information identifying the stored communications to be preserved and the relationship between those communications and the serious foreign contravention; and
(e) specify any information the foreign country has that identifies the carrier that holds the stored communications; and
(f) if the stored communications relate to a specified person—specify any information the foreign country has that identifies the telecommunications service to which the stored communications relate; and

(g) specify the reasons why the stored communications need to be preserved; and

(h) specify that the foreign country intends to make a request under paragraph 15B(d) of the *Mutual Assistance in Criminal Matters Act1987* to access the stored communications.

107Q When a foreign preservation notice is in force

A foreign preservation notice:

(a) comes into force when the carrier receives it; and

(b) ceases to be in force at the earlier of the following times:

(i) if the notice is revoked under section 107R—when the carrier receives notice of the revocation;

(ii) if a stored communications warrant authorising access to the stored communications covered by the notice is issued after the Attorney-General has given an authorisation in relation to the warrant under section 15B of the *Mutual Assistance in Criminal Matters Act1987*—when the warrant ceases to be in force.

107R Revoking a foreign preservation notice

(1) If:

(a) a foreign country makes a request under section 107P to preserve stored communications that are held by a carrier; and

(b) in response to the request, the Australian Federal Police gives a foreign preservation notice to the carrier in relation to those stored communications under subsection107N(1); and

(c) during the period of 180 days starting on the day the carrier was given the notice, the foreign country did not make a request to the Attorney-General under paragraph 15B(d) of the *Mutual Assistance in Criminal Matters Act 1987* to arrange for access to those communications;

then the Australian Federal Police must, by the third working day after the end of that period, revoke the preservation notice by giving the carrier to whom it was given written notice of the revocation.

(2) If:

(a) a foreign country makes a request under section 107P to preserve stored communications that are held by a carrier; and

(b) in response to the request, the Australian Federal Police gives a foreign preservation notice to the carrier in relation to those stored communications under subsection107N(1); and

(c) the foreign country makes a request to the Attorney-General under paragraph 15B(d) of the *Mutual Assistance in Criminal Matters Act 1987* to arrange for access to those communications; and

(d) the Attorney-General refuses that request;

then the Australian Federal Police must, by the third working day after it is notified of the refusal, revoke the preservation notice by giving the carrier to whom it was given written notice of the revocation.

(3) If:

(a) a foreign country makes a request under section 107P to preserve stored communications that are held by a carrier; and

(b) in response to the request, the Australian Federal Police gives a foreign preservation notice to the carrier in relation to those stored communications under subsection107N(1); and

(c) the foreign country withdraws the request;

then the Australian Federal Police must, by the third working day after it is notified of the withdrawal, revoke the preservation notice by giving the carrier to whom it was given written notice of the revocation.

107S Persons who act on the AFP's behalf

A foreign preservation notice must be given or revoked on behalf of the Australian Federal Police by an authorised officer of the Australian Federal Police.

Division 4—Provisions relating to preservation notices

107T Evidentiary certificates relating to actions by carriers

(1) The following:

(a) the Managing Director of a carrier or a body corporate of which the carrier is a subsidiary;

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

(c) an employee of a carrier authorised in writing for the purposes of this paragraph by a person referred to in paragraph (a) or (b);

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 comply with a preservation notice.

(2) A document purporting to be a certificate issued under subsection (1) and purporting to be signed by a person referred to in paragraph (a), (b) or (c) of that subsection:

(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*.

107U Evidentiary certificates relating to actions by issuing agencies

(1) A certifying official of an issuing agency may issue a written certificate signed by him or her setting out such facts as he or she considers relevant with respect to anything done by an officer or staff member of the agency in connection with a preservation notice.

(2) A document purporting to be a certificate issued under this section by a certifying official of an issuing agency and purporting 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 facieevidence of the matters stated in the document.

107V Certified copies of preservation notices

A document certified in writing by a certifying official of an issuing agency to be a true copy of a preservation notice is to be received in evidence in an exempt proceeding as if it were the original preservation notice.

107W How notices are to be given to carriers

For the purposes of this Part:

(a) a preservation notice; or

(b) a revocation notice under section 107L or 107R;

may only be given to a carrier by giving it to an authorised representative of the carrier.

19 Before subparagraph 108(2)(f)(i)

Insert:

(ia) preservation notices; or

20 Division 1 of Part 3-4 (heading)

Repeal the heading, substitute:

Division 1—Prohibition on dealing with accessed information etc.

21 After subparagraph 133(1)(b)(ii)

Insert:

(iia) preservation notice information; or

Note: The heading to section 133 is altered by omitting "**or stored communications warrant information**" and substituting "**etc.**".

22 Section 134

Repeal the section, substitute:

134 Dealing in preservation notice information or stored communications warrant information

A person may, for the purposes of Part 3-1A, 3-2, 3-3, 3-5 or 3-6:

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

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

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

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

23 After subsection 135(4)

Insert:

Preservation notice information

(4A) 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, preservation notice 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 the carrier to comply with the preservation notice.

(4B) An employee of a carrier may communicate or cause to be communicated to another carrier, or to an employee of another carrier, preservation notice information if the information is reasonably necessary to enable the carrier to comply with the preservation notice.

24 After paragraphs 136(1)(a), 137(1)(a), 138(1)(a), 138(2)(a) and 139(1)(a)

Insert:

(aa) preservation notice information;

25 Subsection 146(2)

After “give”, insert “preservation notice information or”.

26 Part 3-5 (heading)

Repeal the heading, substitute:

Part 3-5—Keeping and inspection of preservation notice and access records

27 Division 1 of Part 3-5 (heading)

Repeal the heading, substitute:

Division 1—Keeping preservation notice and access records

28 Before section 151

Insert into Division 1 of Part 3-5:

150A Enforcement agencies to keep documents connected with giving preservation notices

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

(a) each preservation notice given by the agency; and

(b) each instrument revoking such a notice; and

(c) a copy of each certificate issued under subsection 107U(1) by a certifying officer of the agency.

29 Division 2 of Part 3-5 (heading)

Repeal the heading, substitute:

Division 2—Inspection of preservation notice and access records by Ombudsman

30 Paragraph 152(a)

After "150", insert ", 150A".

31 Subsection 153(3)

After "150", insert ", 150A".

32 At the end of Part 3-5

Add:

Division 3—Inspection of preservation notice records by Inspector-General of Intelligence and Security

158A Functions of the Inspector-General of Intelligence and Security

(1) Under the *Inspector-General of Intelligence and Security Act 1986*, the Inspector-General of Intelligence and Security has functions in relation to preservation notices given by the Organisation.

(2) In particular, the Inspector-General of Intelligence and Security has the function of:

(a) inquiring into any matter that relates to compliance by the Organisation with this Act (see subparagraph 8(1)(a)(i) of that Act); and

(b) conducting such inspections of the Organisation as the Inspector-General considers appropriate for the purpose of giving effect to the objects of that Act (see section 9A of that Act).

33 After section 161

Insert:

161A Report to contain information about preservation notices

Domestic preservation notices

(1) The report must set out, for each enforcement agency:

(a) the relevant statistics about domestic preservation notices that were given by the agency during that year; and

(b) the relevant statistics about revocation notices given by the agency under section 107L during that year.

Foreign preservation notices

(2) If the enforcement agency is the Australian Federal Police, the report must also set out:

(a) the relevant statistics about foreign preservation notices that were given by the agency during that year; and

(b) the relevant statistics about revocation notices given by the agency under section 107R during that year.

34 Transitional provision for item 18—ongoing domestic preservation notices

Despite the insertion of section 107H into the *Telecommunications (Interception and Access) Act 1979* made by item 18 of this Schedule, an issuing agency may not a give a carrier an ongoing domestic preservation notice under that section before the end of the period that:

(a) starts on the day this Act receives the Royal Assent; and

(b) ends 90 days after that day.

Schedule 2—Amendments relating to Mutual Assistance

Part 1—Stored communications

Mutual Assistance in Criminal Matters Act 1987

1 Subsection 3(1)

Insert:

> ***carrier*** has the same meaning as in the *Telecommunications (Interception and Access) Act 1979*.

2 Subsection 3(1)

Insert:

> ***investigative proceeding***means a proceeding covered by paragraph (a) or (b) of the definition of ***proceeding***.

3 Subsection 3(1)

Insert:

> ***stored communication*** has the same meaning as in the *Telecommunications (Interception and Access) Act 1979*.

4 After Part III

Insert:

Part IIIA—Assistance in relation to stored communications

15B Requests by foreign countries for stored communications

> The Attorney-General may, in his or her discretion, authorise the Australian Federal Police or a police force or police service of a State, in writing, to apply for a stored communications warrant

under section 110 of the *Telecommunications (Interception and Access) Act 1979* if the Attorney-General is satisfied that:

(a) an investigation, or investigative proceeding, relating to a criminal matter involving an offence against the law of a foreign country (the ***requesting country***) has commenced in the requesting country; and

(b) the offence to which the investigation, or investigative proceeding, relates is punishable by a maximum penalty of:

(i) imprisonment for 3 years or more, imprisonment for life or the death penalty; or

(ii) a fine of an amount that is at least equivalent to 900 penalty units; and

(c) there are reasonable grounds to believe that stored communications relevant to the investigation, or investigative proceeding, are held by a carrier; and

(d) the requesting country has requested the Attorney-General to arrange for access to the stored communications.

Note: Information obtained under the warrant may only be communicated to the requesting country on certain conditions: see subsection 142A(1) of the *Telecommunications (Interception and Access) Act 1979*.

Telecommunications (Interception and Access) Act 1979

5 Subsection 5(1)

Insert:

investigative proceeding has the same meaning as in the *Mutual Assistance in Criminal Matters Act 1987*.

6 Subsection 5(1)

Insert:

mutual assistance application means an application for a stored communications warrant made as a result of an authorisation under section 15B of the *Mutual Assistance in Criminal Matters Act 1987*.

7 After section 5E

Insert:

5EA Serious foreign contraventions

For the purposes of this Act, a ***serious foreign contravention*** is a contravention of a law of a foreign country that is punishable by a maximum penalty of:

(a) imprisonment for 3 years or more, imprisonment for life or the death penalty; or

(b) a fine of an amount that is at least equivalent to 900 penalty units.

8 Paragraph 6H(c)

Omit "paragraph 116(1)(d)", substitute "subparagraph 116(1)(d)(i) or (ii), as the case requires".

9 Paragraph 116(1)(d)

Omit all the words after "with", substitute:

: (i) in the case of an application other than a mutual assistance application—the investigation by the agency of a serious contravention in which the person is involved (including as a victim of the serious contravention); or

(ii) in the case of a mutual assistance application—the investigation or investigative proceeding, by the foreign country to which the application relates, of a serious foreign contravention to which the application relates and in which the person is involved (including as a victim of the serious foreign contravention); and

10 Paragraph 116(1)(e)

After "subsection (2)", insert "or (2A) (as the case requires)".

11 Subsection 116(2)

Omit "The matters", substitute "In the case of an application other than a mutual assistance application, the matters".

12 Paragraph 116(2)(c)

Omit "paragraph (1)(d)", substitute "subparagraph (1)(d)(i)".

13 After subsection 116(2)

Insert:

(2A) In the case of a mutual assistance application, 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 foreign contravention; and

(c) how much the information referred to in subparagraph (1)(d)(ii) would be likely to assist in connection with the investigation, to the extent that this is possible to determine from information obtained from the foreign country to which the application relates.

14 Subsection 116(3)

After "contravention", insert "or serious foreign contravention, but cannot relate to both a serious contravention and a serious foreign contravention".

15 Subsection 118(3)

After "contravention", insert "or serious foreign contravention".

16 Subsection 118(3)

Omit "paragraph 116(1)(d)", substitute "subparagraph 116(1)(d)(i) or (ii), as the case may be".

17 Subsection 139(1)

After "(2)", insert "or (4A)".

18 Subsection 139(2)

Omit "The", substitute "In the case of information obtained by the agency other than through the execution of a warrant issued as a result of a mutual assistance application, the".

19 After subsection 139(4)

Insert:

(4A) In the case of information obtained by the agency through the execution of a warrant issued as a result of a mutual assistance application, the purposes are purposes connected with:

(a) providing the information to the foreign country, or an appropriate authority of the foreign country, to which the application relates; or

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

20 After section 142

Insert:

142A Communicating information obtained as a result of a mutual assistance application to foreign country

(1) Despite subsection 139(4A) and section 142, a person may only communicate information, obtained through the execution of a warrant issued as a result of a mutual assistance application, to the foreign country to which the application relates, subject to the following conditions:

(a) that the information will only be used for the purposes for which the foreign country requested the information;

(b) that any document or other thing containing the information will be destroyed when it is no longer required for those purposes;

(c) any other condition determined, in writing, by the Attorney-General.

(2) A determination made under paragraph (1)(c) is not a legislative instrument.

21 At the end of subsection 162(1)

Add:

; and (c) the relevant statistics about mutual assistance applicationsthat the agency made during that year; and

(d) for each offence (the ***foreign offence***) against a law of a foreign country in respect of which a stored communications warrant was issued as a result of a mutual assistance application made by the agency during the year—the offence (if any), under a law of the Commonwealth, or of a State or a Territory, that is of the same nature as, or a substantially similar nature to, the foreign offence.

22 After paragraph 162(2)(b)

Insert:

(ba) the relevant statistics about mutual assistance applications that were made during that year; and

23 At the end of subsection 162(2)

Add:

; and (e) for each offence (the ***foreign offence***) against a law of a foreign country in respect of which a stored communications warrant was issued as a result of a mutual assistance application made during the year—the offence (if any), under a law of the Commonwealth, or of a State or a Territory, that is of the same nature as, or a substantially similar nature to, the foreign offence.

24 Application of amendments made by this Part

The amendments made by this Part apply in relation to a request by a foreign country that is under consideration on or after the commencement of this item, whether the request was made before or after that commencement.

Part 2—Telecommunications data

Mutual Assistance in Criminal Matters Act 1987

25 Subsection 3(1)

Insert:

communication has the same meaning as in the *Telecommunications (Interception and Access) Act 1979.*

26 Subsection 3(1)

Insert:

telecommunications system has the same meaning as in the *Telecommunications (Interception and Access) Act 1979.*

27 Before Part IV

Insert:

Part IIIB—Assistance in relation to telecommunications data

15D Requests by foreign countries for telecommunications data

(1) This section applies if:

(a) a foreign country requests the disclosure of specified information or specified documents that come into existence during a specified period; and

(b) the information or documents relate to the fact of a communication passing over a telecommunications system.

(2) To avoid doubt, information or documents do not relate to the fact of a communication passing over a telecommunications system:

(a) if the information is the contents or substance of a communication; or

(b) to the extent that the documents contain the contents or substance of a communication.

(3) The Attorney-General may authorise the making of an authorisation under section 180B of the *Telecommunications (Interception and Access) Act 1979*, of a disclosure of information or documents to which this section applies, if he or she is satisfied that:

(a) an investigation relating to a criminal matter involving an offence against the law of the foreign country has commenced in that country; and

(b) the offence:

(i) is punishable by imprisonment for 3 years or more, imprisonment for life or the death penalty; or

(ii) involves an act or omission that, if it had occurred in Australia, would have constituted a serious offence within the meaning of section 5D of the *Telecommunications (Interception and Access) Act 1979*.

Telecommunications Act 1997

28 Subsection 305(1)

After "Division 4", insert "or 4A".

29 Subparagraph 306(1)(b)(ii)

Omit "or subsection 180(3)", substitute ", subsection 180(3) or section 180A".

30 Paragraph 306A(1)(b)

After "section 180", insert "or 180B".

31 Paragraph 306A(1)(b)

After "subsection 180(2)", insert "or 180B(2)".

Telecommunications (Interception and Access) Act 1979

32 Subsection 5(1) (definition of *authorised officer*)

Repeal the definition, substitute:

authorised officer:

(a) in sections 180A, 180B, 180C and 180D, subsections 184(5) and 185(2) and paragraph 186(1)(ca), means:
  (i) the Commissioner of Police; or
  (ii) a Deputy Commissioner of Police; or
  (iii) a member of the Australian Federal Police who is covered by an authorisation in force under subsection 5AB(1A); and
(b) in any other case, means:
  (i) the head (however described) of the enforcement agency or a person acting as that head; or
  (ii) a deputy head (however described) of the enforcement agency or a person acting as that deputy head; or
  (iii) a person who holds, or is acting in, an office or position in the enforcement agency that is covered by an authorisation in force under subsection 5AB(1).

33 Subsection 5(1)

Insert:

foreign law enforcement agency means:
(a) a police force (however described) of a foreign country; or
(b) any other authority or person responsible for the enforcement of the laws of the foreign country.

34 Subsection 5AB(1)

Omit "paragraph (c)", substitute "subparagraph (b)(iii)".

Note: The following heading to subsection 5AB(1) is inserted "*Authorised officers of an enforcement agency*".

35 Subsection 5AB(2)

Repeal the subsection, substitute:

Authorised officers of the Australian Federal Police

(1A) The Commissioner of Police may authorise, in writing, a senior executive AFP employee who is a member of the Australian Federal Police to be an authorised officer.

(2) A copy of an authorisation must be given to the Communications Access Coordinator:

(a) in the case of an authorisation made under subsection (1)—by the head of the enforcement agency; and

(b) in the case of an authorisation made under subsection (1A)—by the Commissioner of Police.

36 Subsection 171(1)

Omit "and 4", substitute ", 4 and 4A".

37 Subsection 171(1) (note 1)

Repeal the note, substitute:

Note 1: Division 3 covers the Organisation. Division 4 covers disclosures for the purposes of Australian enforcement agencies. Division 4A covers disclosures for the purposes of foreign law enforcement.

38 At the end of subsection 171(3)

Add "or 4A".

39 Section 172

Omit "and 4", substitute ", 4 and 4A".

40 Subsection 180(5)

Repeal the subsection.

41 After Division 4 of Part 4-1

Insert:

Division 4A—Foreign law enforcement

Subdivision A—Primary disclosures

180A Authorisations for access to existing information or documents—enforcement of the criminal law of a foreign country

Disclosure to the Australian Federal Police

(1) Sections 276, 277 and 278 of the *Telecommunications Act 1997* do not prevent a disclosure of information or a document if the information or document is covered by an authorisation in force under subsection (2).

(2) An authorised officer of the Australian Federal Police may authorise the disclosure of specified information or specified documents that came into existence before the time the person from whom the disclosure is sought receives notification of the authorisation.

Note: Section 184 deals with notification of authorisations.

(3) The authorised officer must not make the authorisation unless he or she is satisfied that the disclosure is reasonably necessary for the enforcement of the criminal law of a foreign country.

Disclosure to a foreign law enforcement agency

(4) If specified information or specified documents are disclosed because of an authorisation given under subsection (2), an authorised officer of the Australian Federal Police may authorise the disclosure of the information or documents so disclosed to a foreign law enforcement agency.

(5) The authorised officer must not make the authorisation unless he or she is satisfied that:

(a) the disclosure is reasonably necessary for the enforcement of the criminal law of a foreign country; and

(b) the disclosure is appropriate in all the circumstances.

180B Authorisations for access to prospective information or documents—enforcement of the criminal law of a foreign country

Disclosure to the Australian Federal Police

(1) Sections 276, 277 and 278 of the *Telecommunications Act 1997* do not prevent a disclosure of information or a document if the information or document is covered by an authorisation in force under subsection (2) of this section.

Prospective authorisation

(2) An authorised officer of the Australian Federal Police may authorise the disclosure of specified information or specified documents that come into existence during the period for which the authorisation is in force.

(3) The authorised officer must not make the authorisation unless:

(a) the Attorney-General has authorised the making of the authorisation under the *Mutual Assistance in Criminal Matters Act 1987*; and

(b) the authorised officer is satisfied that the disclosure is reasonably necessary for the investigation of an offence against the law of a foreign country that:

(i) is punishable by imprisonment for 3 years or more, imprisonment for life or the death penalty; or

(ii) involves an act or omission that, if it had occurred in Australia, would have constituted a serious offence within the meaning of section 5D of the *Telecommunications (Interception and Access) Act 1979*; and

(c) the authorised officer is satisfied that the disclosure is appropriate in all the circumstances.

(4) An authorised officer of the Australian Federal Police must revoke the authorisation if he or she is satisfied that the disclosure is no longer required.

Note: Section 184 deals with notification of revocations.

(5) An authorisation under subsection (2):

(a) comes into force at the time the person from whom the disclosure is sought receives notification of the authorisation; and

(b) ceases to be in force at the time specified in the authorisation, which must not be more than 21 days after the day the authorisation is made, or that period as extended under subsection (6), unless it is revoked earlier.

Note: Section 184 deals with notification of authorisations.

Extension of prospective authorisation

(6) The period for which an authorisation under subsection (2) is in force may be extended once only, by an authorised officer of the Australian Federal Police, if the authorised officer is satisfied that the extension is:

(a) reasonably necessary for the investigation of an offence against the law of a foreign country that:

(i) is punishable by imprisonment for 3 years or more, imprisonment for life or the death penalty; or

(ii) involves an act or omission that, if it had occurred in Australia, would have constituted a serious offence within the meaning of section 5D of the *Telecommunications (Interception and Access) Act 1979*; and

(b) appropriate in all the circumstances.

(7) An extension under subsection (6) must not be for more than 21 days from the day of the extension.

Disclosure to a foreign law enforcement agency

(8) If specified information or specified documents are disclosed because of an authorisation given under subsection (2), an authorised officer of the Australian Federal Police may authorise the disclosure of the information or documents so disclosed to a foreign law enforcement agency if the authorised officer is satisfied that the disclosure is:

(a) reasonably necessary for the investigation of an offence against the law of a foreign country that:

(i) is punishable by imprisonment for 3 years or more, imprisonment for life or the death penalty; or

(ii) involves an act or omission that, if it had occurred in Australia, would have constituted a serious offence within the meaning of section 5D of the *Telecommunications (Interception and Access) Act 1979*; and

(b) appropriate in all the circumstances.

(9) An authorised officer must not make more than one authorisation a day under subsection (8).

Subdivision B—Secondary disclosures

180C Authorisations to disclose information or documents—enforcement of the criminal law of a foreign country

(1) If specified information or specified documents are disclosed because of an authorisation given under Division 4, other than because of an authorisation under section 178A (missing persons),

an authorised officer of the Australian Federal Police may authorise the disclosure of the information or documents so disclosed to a foreign law enforcement agency.

(2) The authorised officer must not make the authorisation unless he or she is satisfied that:

(a) the disclosure is reasonably necessary for the enforcement of the criminal law of a foreign country; and

(b) the disclosure is appropriate in all the circumstances.

180D Authorisations to disclose information or documents—enforcement of the criminal law

(1) If specified information or specified documents are disclosed because of an authorisation given under this Division, an authorised officer of the Australian Federal Police may authorise the following:

(a) the disclosure of the information or documents to the Organisation or an enforcement agency;

(b) the use of the information or documents by the Australian Federal Police.

(2) The authorised officer must not make the authorisation unless he or she is satisfied that:

(a) in the case of a disclosure to the Organisation—the disclosure is reasonably necessary for the performance by the Organisation of its functions; and

(b) in the case of a disclosure to an enforcement agency—the disclosure is reasonably necessary:

(i) for the enforcement of the criminal law; or

(ii) for the enforcement of a law imposing a pecuniary penalty; or

(iii) for the protection of the public revenue; and

(c) in the case of a use by the Australian Federal Police—the use is reasonably necessary:

(i) for the enforcement of the criminal law; or

(ii) for the enforcement of a law imposing a pecuniary penalty; or

(iii) for the protection of the public revenue; and

(d) in any case—the disclosure or use is appropriate in all the circumstances.

Subdivision C—Conditions of disclosure to foreign country

180E Disclosing information etc. obtained to foreign country

(1) A person must not disclose information or a document in accordance with an authorisation under section 180A, 180B or 180C to a foreign country unless the disclosure is subject to the following conditions:

(a) that the information will only be used for the purposes for which the foreign country requested the information;

(b) that any document or other thing containing the information will be destroyed when it is no longer required for those purposes;

(c) in the case of information or a document disclosed under section 180B—any other condition determined, in writing, by the Attorney-General.

(2) A determination made under paragraph (1)(c) is not a legislative instrument.

Division 4B—Privacyto be considered when making authorisations

180F Authorised officers to consider privacy

Before making an authorisation under Division 4 or 4A in relation to the disclosure or use of information or documents, the authorised officer considering making the authorisation must have regard to whether any interference with the privacy of any person or persons that may result from the disclosure or use is justifiable, having regard to the following matters:

(a) the likely relevance and usefulness of the information or documents;

(b) the reason why the disclosure or use concerned is proposed to be authorised.

42 Paragraph 181(b)

Omit “or 4”, substitute “, 4 or 4A”.

43 Paragraph 182(1)(a)

After "Division 4", insert "or 4A".

44 After subsection 182(4)

Insert:

(4A) Paragraph (1)(b) does not apply to a disclosure or use of information or a document if the disclosure or use is permitted by section 180C or 180D.

Note: A defendant bears an evidential burden in relation to the matter in subsection (4A) (see subsection 13.3(3) of the *Criminal Code*).

45 Subsection 182(5) (definition of *non-missing person information*)

After "Division 4", insert "or 4A".

46 Paragraph 183(1)(a)

Omit "or 4", substitute ", 4 or 4A".

47 At the end of section 184

Add:

Authorised officers of the Australian Federal Police

(5) If an authorised officer of the Australian Federal Police makes an authorisation under subsection 180A(2) or 180B(2), or extends the period for which an authorisation is in force under subsection 180B(6), a relevant staff member of the Australian Federal Police must notify the person from whom the disclosure is sought.

(6) If, under subsection 180B(4), an authorised officer of the Australian Federal Police revokes an authorisation, a relevant staff member of the Australian Federal Police must notify the person who was notified of the authorisation.

48 Section 185

Before "The", insert "(1)".

49 At the end of section 185

Add:

(2) The Commissioner of Police must retain an authorisation made under Division 4A of Part 4-1 by an authorised officer of the Australian Federal Police for the period of 3 years beginning on the day the authorisation is made.

50 After paragraph 186(1)(c)

Insert:

(ca) if the enforcement agency is the Australian Federal Police—the number of authorisations made under sections 180A, 180B, 180C and 180D by an authorised officer of the Australian Federal Police during that year; and

(cb) if the enforcement agency is the Australian Federal Police, and information or documents were disclosed, under an authorisation referred to in paragraph (ca), by an authorised officer of the Australian Federal Police during that year to one or more foreign countries:

(i) the name of each such country; and

(ii) the number of disclosures under such authorisations; and

50A Subsection 186(2)

After "subsection (1)", insert ", other than the information referred to in paragraph (1)(cb)".

51 Application of amendments made by this Part—authorisations

(1) The amendments made by this Part apply in relation to an authorisation made on or after the commencement of this item.

(2) To avoid doubt, an authorisation may be made under section 180C of the *Telecommunications (Interception and Access) Act 1979* even if an authorisation given under Division 4 (as mentioned in that section) was given before the commencement of this item.

52 Application of amendments made by this Part—requests by foreign countries

The amendments made by this Part apply in relation to a request by a foreign country that is under consideration on or after the commencement of this item, whether the request was made before or after that commencement.

53 Saving of existing authorisations

(1) Despite the amendment of subsection 5AB(1) of the *Telecommunications (Interception and Access) Act 1979* by this Part, any authorisation by the head of an enforcement agency that was in force under that subsection immediately before the commencement of this item continues in force on and after that commencement as if it were an authorisation made under that subsection as in force after that commencement.

(2) In this item:

enforcement agency has the same meaning as in the *Telecommunications (Interception and Access) Act 1979.*

Part 3—Recovery of costs by carriage service providers etc. for providing assistance to Australian law enforcement authorities

Telecommunications Act 1997

54 After paragraph 313(3)(c)

Insert:

(ca) assisting the enforcement of the criminal laws in force in a foreign country;

55 After paragraph 313(4)(c)

Insert:

(ca) assisting the enforcement of the criminal laws in force in a foreign country;

56 Application of amendments made by items 54 and 55

(1) The amendment made by item 54 of this Schedule applies to help given by a carrier or carriage service provider on or after the commencement of this item.

(2) The amendment made by item 55 of this Schedule applies to help given by a carriage service intermediary on or after the commencement of this item.

Schedule 3—Computer offences amendments

Criminal Code Act 1995

1 Subsection 476.1(1) of the *Criminal Code* (definition of *Commonwealth computer*)

Repeal the definition.

2 Paragraph 477.1(1)(b) of the *Criminal Code*

Repeal the paragraph.

3 Subsection 477.1(2) of the *Criminal Code*

Repeal the subsection.

4 Subsections 477.1(4) and (5) of the *Criminal Code*

Repeal the subsections.

5 Subparagraph 477.2(1)(c)(ii) of the *Criminal Code*

Omit "data; and", substitute "data.".

6 Paragraph 477.2(1)(d) of the *Criminal Code*

Repeal the paragraph.

7 Subsection 477.2(2) of the *Criminal Code*

Repeal the subsection.

8 Paragraph 477.3(1)(b) of the *Criminal Code*

Omit "unauthorised; and", substitute "unauthorised.".

9 Paragraph 477.3(1)(c) of the *Criminal Code*

Repeal the paragraph.

10 Subsection 477.3(2) of the *Criminal Code*

Repeal the subsection.

11 Paragraph 478.1(1)(c) of the *Criminal Code*

Omit “unauthorised; and”, substitute “unauthorised.”.

12 Paragraph 478.1(1)(d) of the *Criminal Code*

Repeal the paragraph.

13 Subsection 478.1(2) of the *Criminal Code*

Repeal the subsection.

14 Subsection 478.2(1) of the *Criminal Code*

Omit “(1)”.

15 Paragraph 478.2(1)(c) of the *Criminal Code*

Omit “unauthorised; and”, substitute “unauthorised.”.

16 Paragraph 478.2(1)(d) of the *Criminal Code*

Repeal the paragraph.

17 Subsection 478.2(2) of the *Criminal Code*

Repeal the subsection.

18 Application of amendments

The amendments made by this Schedule apply to acts and omissions that take place after the day on which this Schedule commences.

Schedule 4—Telecommunications data confidentiality

Telecommunications (Interception and Access) Act 1979

1 Subsection 171(3)

Repeal the subsection, substitute:

(3) Division 6 creates offences for certain disclosures and uses of information and documents.

2 Division 6 of Part 4-1 (heading)

Repeal the heading, substitute:

Division 6—Disclosure/use offences

3 Before section 182

Insert:

181A Disclosure/use offences: authorisations under Division 3

Disclosures

(1) A person commits an offence if:
  (a) the person discloses information; and
  (b) the information is about any of the following:
    (i) whether an authorisation under Division 3 has been, or is being, sought;
    (ii) the making of such an authorisation;
    (iii) the existence or non-existence of such an authorisation;
    (iv) the revocation of such an authorisation;
    (v) the notification of such a revocation.

Penalty: Imprisonment for 2 years.

(2) A person commits an offence if:
  (a) the person discloses a document; and

(b) the document consists (wholly or partly) of any of the following:
(i) an authorisation under Division 3;
(ii) the revocation of such an authorisation;
(iii) the notification of such a revocation.

Penalty: Imprisonment for 2 years.

(3) Paragraphs (1)(a) and (2)(a) do not apply to a disclosure of information or a document if:
(a) the disclosure is for the purposes of the authorisation, revocation or notification concerned; or
(b) the disclosure is reasonably necessary:
(i) to enable the Organisation to perform its functions; or
(ii) to enforce the criminal law; or
(iii) to enforce a law imposing a pecuniary penalty; or
(iv) to protect the public revenue.

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

Uses

(4) A person commits an offence if:
(a) the person uses information; and
(b) the information is about any of the following:
(i) whether an authorisation under Division 3 has been, or is being, sought;
(ii) the making of such an authorisation;
(iii) the existence or non-existence of such an authorisation;
(iv) the revocation of such an authorisation;
(v) the notification of such a revocation.

Penalty: Imprisonment for 2 years.

(5) A person commits an offence if:
(a) the person uses a document; and
(b) the document consists (wholly or partly) of any of the following:
(i) an authorisation under Division 3;
(ii) the revocation of such an authorisation;

(iii) the notification of such a revocation.

Penalty: Imprisonment for 2 years.

(6) Paragraphs (4)(a) and (5)(a) do not apply to a use of information or a document if:

(a) the use is for the purposes of the authorisation, revocation or notification concerned; or

(b) the use is reasonably necessary:

(i) to enable the Organisation to perform its functions; or

(ii) to enforce the criminal law; or

(iii) to enforce a law imposing a pecuniary penalty; or

(iv) to protect the public revenue.

Note: A defendant bears an evidential burden in relation to the matter in subsection (6) (see subsection 13.3(3) of the *Criminal Code*).

181B Disclosure/use offences: certain authorisations under Division 4

Disclosures

(1) A person commits an offence if:

(a) the person discloses information; and

(b) the information is about any of the following:

(i) whether an authorisation under Division 4 (other than under section 178A) has been, or is being, sought;

(ii) the making of such an authorisation;

(iii) the existence or non-existence of such an authorisation;

(iv) the revocation of such an authorisation;

(v) the notification of such a revocation.

Penalty: Imprisonment for 2 years.

(2) A person commits an offence if:

(a) the person discloses a document; and

(b) the document consists (wholly or partly) of any of the following:

(i) an authorisation under Division 4 (other than under section 178A);

(ii) the revocation of such an authorisation;

(iii) the notification of such a revocation.

Penalty: Imprisonment for 2 years.

(3) Paragraphs (1)(a) and (2)(a) do not apply to a disclosure of information or a document if:

(a) the disclosure is for the purposes of the authorisation, revocation or notification concerned; or

(b) the disclosure is reasonably necessary:

(i) to enable the Organisation to perform its functions; or

(ii) to enforce the criminal law; or

(iii) to enforce a law imposing a pecuniary penalty; or

(iv) to protect the public revenue.

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

Uses

(4) A person commits an offence if:

(a) the person uses information; and

(b) the information is about any of the following:

(i) whether an authorisation under Division 4 (other than under section 178A) has been, or is being, sought;

(ii) the making of such an authorisation;

(iii) the existence or non-existence of such an authorisation;

(iv) the revocation of such an authorisation;

(v) the notification of such a revocation.

Penalty: Imprisonment for 2 years.

(5) A person commits an offence if:

(a) the person uses a document; and

(b) the document consists (wholly or partly) of any of the following:

(i) an authorisation under Division 4 (other than under section 178A);

(ii) the revocation of such an authorisation;

(iii) the notification of such a revocation.

Penalty: Imprisonment for 2 years.

(6) Paragraphs (4)(a) and (5)(a) do not apply to a use of information or a document if:

(a) the use is for the purposes of the authorisation, revocation or notification concerned; or

(b) the use is reasonably necessary:

(i) to enforce the criminal law; or

(ii) to enforce a law imposing a pecuniary penalty; or

(iii) to protect the public revenue.

Note: A defendant bears an evidential burden in relation to the matter in subsection (6) (see subsection 13.3(3) of the *Criminal Code*).

Note: The heading to section 182 is altered by adding at the end "**: disclosures under Division 4**".

4 Application

Sections 181A and 181B of the *Telecommunications (Interception and Access) Act 1979* apply in relation to a disclosure, or use, of information or a document on or after the commencement of this Schedule whether the information or document came into existence before, on or after that commencement.

Schedule 5—Miscellaneous

Telecommunications (Interception and Access) Act 1979

1 At the end of section 105

Add:

(5) Section 15.1 (extended geographical jurisdiction—category A) of the *Criminal Code* applies to an offence against subsection 7(1) or section 63.

3 Subsection 180(4)

Omit all the words after "reasonably necessary", substitute:

for the investigation of:

(a) a serious offence; or

(b) an offence against a law of the Commonwealth, a State or a Territory that is punishable by imprisonment for at least 3 years.

4 Application of amendments made by items 1 and 3

(1) The amendment made by item 1 of this Schedule applies to acts or things done on or after the day this Schedule commences.

(2) The amendment made by item 3 of this Schedule applies in relation to an authorisation made on or after the day this Schedule commences.

[*Minister's second reading speech made in—*
House of Representatives on 22 June 2011
Senate on 24 August 2011]

(114/11)