Telecommunications (Interception and Access) Amendment Act 2007

No. 177, 2007

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

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

Contents

Telecommunications (Interception and Access) Amendment Act 2007

No. 177, 2007

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

[*Assented to 28 September 2007*]

The Parliament of Australia enacts:

1 Short title

This Act may be cited as the *Telecommunications (Interception and Access) Amendment Act 2007*.

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 on which this Act receives the Royal Assent.	28 September 2007
2. Schedule 1	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.	1 November 2007 (*see* F2007L03941)
3. Schedule 2, item 1	Immediately after the time specified in the *Telecommunications (Interception) Amendment Act 2006* for the commencement of item 8 of Schedule 5 to that Act.	3 November 2006
4. Schedule 2, items 2 to 26	The day after this Act receives the Royal Assent.	29 September 2007

Note: This table relates only to the provisions of this Act as originally passed by both Houses of 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Each Act that is specified in a Schedule to this Act is amended or repealed as set out in the applicable items in the Schedule concerned, and any other item in a Schedule to this Act has effect according to its terms.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—Access to telecommunications data and co-operation with interception agencies

Part 1—Main amendments

Telecommunications (Interception and Access) Act 1979

1 Subsection 5(1)

Insert:

ACMA means the Australian Communications and Media Authority.

2 Subsection 5(1)

Insert:

authorised officer of an enforcement agency means:

(a) the head (however described) of the enforcement agency or a person acting as that head; or

(b) a deputy head (however described) of the enforcement agency or a person acting as that deputy head; or

(c) 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).

3 Subsection 5(1)

Insert:

Communications Access Co-ordinator has the meaning given by section 6R.

4 Subsection 5(1)

Insert:

criminal law-enforcement agency means a body covered by any of paragraphs (a) to (k) of the definition of ***enforcement agency*** in this subsection.

5 Subsection 5(1)

Insert:

delivery point means a location in respect of which a nomination or determination is in force under section 188.

6 Subsection 5(1) (definition of *enforcement agency*)

Repeal the definition, substitute:

enforcement agency means:

(a) the Australian Federal Police; or
(b) a police force or service of a State; or
(c) the Australian Commission for Law Enforcement Integrity; or
(d) the ACC; or
(e) the Crime Commission; or
(f) the Independent Commission Against Corruption; or
(g) the Police Integrity Commission; or
(h) the Office of Police Integrity; or
(i) the Crime and Misconduct Commission; or
(j) the Corruption and Crime Commission; or
(k) an authority established by or under a law of the Commonwealth, a State or a Territory that is prescribed by the regulations for the purposes of this paragraph; or
(l) a body or organisation responsible to the Ministerial Council for Police and Emergency Management - Police; or
(m) the CrimTrac Agency; or
(n) any body whose functions include:
  (i) administering a law imposing a pecuniary penalty; or
  (ii) administering a law relating to the protection of the public revenue.

7 Subsection 5(1) (paragraph (a) of the definition of *interception agency*)

Omit "Part 2-6", substitute "section 6R, Part 2-6 or Chapter 5".

8 Subsection 5(1) (at the end of the definition of *interception agency*)

Add:

; or (c) for the purposes of section 6R and Chapter 5:

(i) the Organisation; or

(ii) a Commonwealth agency; or

(iii) an eligible authority of a State in relation to which a declaration under section 34 is in force.

9 Subsection 5(1)

Insert:

relevant staff member of an enforcement agency means:

(a) the head (however described) of the enforcement agency; or

(b) a deputy head (however described) of the enforcement agency; or

(c) any employee, member of staff or officer of the enforcement agency.

10 After section 5AA

Insert:

5AB Authorised officers

(1) The head (however described) of an enforcement agency may, by writing, authorise a management office or management position in the enforcement agency for the purposes of paragraph (c) of the definition of ***authorised officer*** in subsection 5(1).

(2) The head of the enforcement agency must give a copy of an authorisation to the Communications Access Co-ordinator.

Authorisations are not legislative instruments

(3) An authorisation made under this section is not a legislative instrument.

11 At the end of Part 1-2

Add:

6R Communications Access Co-ordinator

(1) In this Act:

Communications Access Co-ordinator means:

(a) the Secretary of the Department; or

(b) if a person or body is covered by an instrument under subsection (2)—that person or body.

(2) The Minister may, by legislative instrument, specify a person or body for the purposes of paragraph (b) of the definition of ***Communications Access Co-ordinator*** in subsection (1).

(3) Unless the context otherwise requires, an act done by or in relation to the Communications Access Co-ordinator is taken to be an act done by or in relation to the Co-ordinator on behalf of all the interception agencies.

12 After Chapter 3

Insert:

Chapter 4—Access to telecommunications data

Part 4-1—Permitted access to telecommunications data

Division 1—Outline of Part

171 Outline of Part

(1) Divisions 3 and 4 set out some circumstances when sections 276, 277 and 278 of the *Telecommunications Act 1997* do not prohibit a disclosure of information or a document.

Note 1: Division 3 covers the Organisation. Division 4 covers enforcement agencies.

Note 2: Those Divisions do not permit the disclosure of the contents or substance of a communication: see Division 2.

(2) Division 5 sets out some circumstances when sections 276, 277 and 278 of the *Telecommunications Act 1997* do not prohibit a use of information or a document.

(3) Division 6 creates an offence for secondary disclosure or use of information or a document that is disclosed as permitted by Division 4.

Division 2—General provisions

172 No disclosure of the contents or substance of a communication

Divisions 3 and 4 do not permit the disclosure of:

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

(b) a document to the extent that the document contains the contents or substance of a communication.

173 Effect of Divisions 3 to 5

Nothing in Divisions 3 to 5 limits the generality of anything else in those Divisions or in Subdivision A of Division 3 of Part 13 of the *Telecommunications Act 1997*.

Division 3—The Organisation

174 Voluntary disclosure

(1) Sections 276, 277 and 278 of the *Telecommunications Act 1997* do not prohibit a disclosure by a person (the ***holder***) of information or a document to the Organisation if the disclosure is in connection with the performance by the Organisation of its functions.

Limitation

(2) This section does not apply if the Director-General of Security, the Deputy Director-General of Security or an officer or employee of the Organisation requests the holder to disclose the information or document.

Note: Sections 175 and 176 deal with the disclosure of information or a document in response to authorisations by the Organisation.

175 Authorisations for access to existing information or documents

(1) Sections 276, 277 and 278 of the *Telecommunications Act 1997* do not prohibit a disclosure of information or a document if the

information or document is covered by an authorisation in force under subsection (2).

Making of authorisation

(2) The following persons (each of whom is an ***eligible person***):
  (a) the Director-General of Security;
  (b) the Deputy Director-General of Security;
  (c) an officer or employee of the Organisation covered by an approval in force under subsection (4);

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 eligible person must not make the authorisation unless he or she is satisfied that the disclosure would be in connection with the performance by the Organisation of its functions.

Approvals

(4) The Director-General of Security may, by writing, approve an officer or employee of the Organisation for the purposes of paragraph (2)(c).

176 Authorisations for access to prospective information or documents

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

Prospective authorisation

(2) The following persons (each of whom is an ***eligible person***):
  (a) the Director-General of Security;
  (b) the Deputy Director-General of Security;
  (c) an officer or employee of the Organisation who holds, or is acting in, a position that is equivalent to, or that is higher than, an SES Band 2 position in the Department;

may authorise the disclosure of specified information or specified documents that come into existence during the period for which the authorisation is in force.

Authorisation for access to existing information or documents may also be sought

(3) The eligible person may, in that authorisation, also authorise the disclosure of specified information or specified documents that came into existence before the time the authorisation comes into force.

Limits on making the authorisation

(4) The eligible person must not make the authorisation unless he or she is satisfied that the disclosure would be in connection with the performance by the Organisation of its functions.

Period for which authorisation is in force

(5) An authorisation under this section:
  (a) comes into force at the time the person from whom the disclosure is sought receives notification of the authorisation; and
  (b) ends at the time specified in the authorisation (which must be a time that is no longer than the end of the period of 90 days beginning on the day the authorisation is made), unless it is revoked earlier.

Note: Section 184 deals with notification of authorisations.

Revoking the authorisation

(6) An eligible person 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.

Division 4—Enforcement agencies

177 Voluntary disclosure

Enforcement of the criminal law

(1) Sections 276, 277 and 278 of the *Telecommunications Act 1997* do not prevent a disclosure by a person (the ***holder***) of information or a document to an enforcement agency if the disclosure is reasonably necessary for the enforcement of the criminal law.

Enforcement of a law imposing a pecuniary penalty or protection of the public revenue

(2) Sections 276 and 277 of the *Telecommunications Act 1997* do not prevent a disclosure by a person (the ***holder***) of information or a document to an enforcement agency if the disclosure is reasonably necessary for the enforcement of a law imposing a pecuniary penalty or for the protection of the public revenue.

Limitation

(3) This section does not apply if a relevant staff member of an enforcement agency requests the holder to disclose the information or document.

Note: Sections 178 to 180 deal with the disclosure of information or a document in response to authorisations by an authorised officer of an enforcement agency.

178 Authorisations for access to existing information or documents—enforcement of the criminal law

(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 an enforcement agency 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.

179 Authorisations for access to existing information or documents—enforcement of a law imposing a pecuniary penalty or protection of the public revenue

(1) Sections 276 and 277 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 an enforcement agency 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 a law imposing a pecuniary penalty or for the protection of the public revenue.

180 Authorisations for access to prospective information or documents

(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 this section.

Prospective authorisation

(2) An authorised officer of a criminal law-enforcement agency may authorise the disclosure of specified information or specified documents that come into existence during the period for which the authorisation is in force.

Authorisation for access to existing information or documents may also be sought

(3) The authorised officer may, in that authorisation, also authorise the disclosure of specified information or specified documents that came into existence before the time the authorisation comes into force.

Limits on making the authorisation

(4) The authorised officer must not make the authorisation unless he or she is satisfied that the disclosure is reasonably necessary for the investigation of an offence against a law of the Commonwealth, a State or a Territory that is punishable by imprisonment for at least 3 years.

(5) Before making the authorisation, the authorised officer must have regard to how much the privacy of any person or persons would be likely to be interfered with by the disclosure.

Period for which authorisation is in force

(6) An authorisation under this section:

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

(b) ends at the time specified in the authorisation (which must be a time that is no longer than the end of the period of 45 days beginning on the day the authorisation is made), unless it is revoked earlier.

Note: Section 184 deals with notification of authorisations.

Revoking the authorisation

(7) An authorised officer of the criminal law-enforcement agency 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.

Division 5—Uses of telecommunications data connected with provision of access

181 Uses of telecommunications data connected with provision of access

Section 276, 277 or 278 of the *Telecommunications Act 1997* does not prohibit a use by a person of information or a document if:

(a) the use is made for the purposes of, or in connection with, a disclosure of the information or document by the person; and

(b) because of Division 3 or 4 of this Part, the disclosure is not prohibited by that section.

Division 6—Secondary disclosure/use offence

182 Secondary disclosure/use offence

(1) A person commits an offence if:

(a) information or a document is disclosed to the person as permitted by Division 4; and

(b) the person discloses or uses the information or document.

Penalty: Imprisonment for 2 years.

Exempt disclosures

(2) Paragraph (1)(b) does not apply to a disclosure of information or a document if the disclosure is reasonably necessary:

(a) for the performance by the Organisation of its functions; or

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

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

(d) for the protection of the public revenue.

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

Exempt uses

(3) Paragraph (1)(b) does not apply to a use of information or a document if the use is reasonably necessary:

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

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

(c) for the protection of 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*).

Part 4-2—Procedural requirements relating to authorisations

183 Form of authorisations and notifications

(1) The following:

(a) an authorisation under Division 3 or 4 of Part 4-1;

(b) the notification of such an authorisation;

(c) the revocation of such an authorisation;

(d) the notification of such a revocation;

must:

(e) be in written form or in electronic form (for example, email); and

(f) comply with such requirements as are determined under subsection (2).

(2) The Communications Access Co-ordinator may, by legislative instrument, determine requirements for the purposes of paragraph (1)(f).

(3) The Co-ordinator must consult the ACMA and the Privacy Commissioner before making a determination under subsection (2).

184 Notification of authorisations or revocations

The Organisation

(1) If a person makes an authorisation under Division 3 of Part 4-1, an officer or employee of the Organisation must notify the person from whom the disclosure is sought.

(2) If, under subsection 176(6), a person revokes an authorisation, an officer or employee of the Organisation must notify the person who was notified of the authorisation.

Enforcement agencies

(3) If an authorised officer of an enforcement agency makes an authorisation under Division 4 of Part 4-1, a relevant staff member of the enforcement agency must notify the person from whom the disclosure is sought.

(4) If, under subsection 180(7), an authorised officer of a criminal law-enforcement agency revokes an authorisation, a relevant staff member of the enforcement agency must notify the person who was notified of the authorisation.

185 Retention of authorisations

The head (however described) of an enforcement agency must retain an authorisation made under Division 4 of Part 4-1 by an authorised officer of the enforcement agency for the period of 3 years beginning on the day the authorisation is made.

186 Report to Minister

(1) As soon as practicable, and in any event within 3 months, after each 30 June, the head (however described) of an enforcement agency must give the Minister a written report that relates to the year ending on that 30 June and that sets out:

(a) the number of authorisations made under section 178 by an authorised officer of the enforcement agency during that year; and

(b) the number of authorisations made under section 179 by an authorised officer of the enforcement agency during that year; and

(c) for a criminal law-enforcement agency—the number of authorisations made under section 180 by an authorised officer of the enforcement agency during that year; and

(d) any other matter requested by the Minister in relation to those authorisations.

(2) The Minister must prepare a report that contains the information set out in each report under subsection (1). The report may contain any other information the Minister considers appropriate.

(3) The Minister must cause a copy of a report under subsection (2) to be laid before each House of the Parliament within 15 sitting days of that House after the day on which the report was completed.

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

Chapter 5—Co-operation with interception agencies

Part 5-1—Definitions

187 Definitions

(1) This section sets out the meaning of the following 2 important concepts used in this Chapter:

(a) interception capability (relating to obligations under Part 5-3);

(b) delivery capability (relating to obligations under Part 5-5).

These concepts do not overlap.

Interception capability

(2) In this Chapter, ***interception capability***, in relation to a particular kind of telecommunications service that involves, or will involve, the use of a telecommunications system, means the capability of that kind of service or of that system to enable:

(a) a communication passing over the system to be intercepted; and

(b) lawfully intercepted information to be transmitted to the delivery points applicable in respect of that kind of service.

Delivery capability

(3) In this Chapter, ***delivery capability***, in relation to a particular kind of telecommunications service that involves, or will involve, the use of a telecommunications system, means the capability of that kind of service or of that system to enable lawfully intercepted

information to be delivered to interception agencies from the delivery points applicable in respect of that kind of service.

Part 5-2—Delivery points

188 Delivery points

(1) Each carrier must:

(a) nominate, in respect of a particular kind of telecommunications service of that carrier and in respect of each interception agency, at least one place in Australia as the location of a point from which lawfully intercepted information can most conveniently be transmitted in relation to that interception agency; and

(b) inform the Communications Access Co-ordinator of the place or places nominated for each interception agency.

Note 1: The nominated location becomes a delivery point: see the definition of ***delivery point*** in subsection 5(1).

Note 2: The definition of ***carrier*** in subsection 5(1) includes carriage service providers.

Note 3: Delivery points are significant for the interception capability obligations in Part 5-3 and for the delivery capability obligations in Part 5-5.

Disagreement over delivery points

(2) The Communications Access Co-ordinator may, at any time, notify a carrier that an interception agency does not agree to the location of a point nominated under subsection (1) by that carrier in respect of a particular kind of telecommunications service and of that interception agency.

(3) Upon being so notified, the carrier must nominate another location of a point in respect of that kind of telecommunications service and of that interception agency and inform the Communications Access Co-ordinator.

Note: The nominated location becomes a delivery point: see the definition of ***delivery point*** in subsection 5(1).

(4) If the location of a point nominated under subsection (3) is still unsatisfactory to the interception agency, the Communications Access Co-ordinator must:
  (a) inform the carrier to that effect; and
  (b) refer the disagreement to the ACMA for a determination under subsection (5).

(5) The ACMA, after hearing the views of the carrier and the views of the interception agency concerning the best location of a point in relation to that kind of telecommunications service and that interception agency, must determine the location of a point for the purposes of this section.

Note: The determined location becomes a delivery point: see the definition of ***delivery point*** in subsection 5(1).

Factors to be considered in determining delivery points

(6) In determining the location of a delivery point, the carrier and the interception agency or, failing agreement, the ACMA, must have regard to:
  (a) the configuration of the kind of telecommunications service in respect of which the delivery point is required to be decided; and
  (b) the relative costs to the carrier and the interception agency of any particular point that is chosen as that delivery point; and
  (c) the reasonable needs of the interception agency; and
  (d) the reasonable commercial requirements of the carrier; and
  (e) the location of any delivery points already existing in relation to that interception agency or other interception agencies.

(7) It is not a requirement that a place where an interception takes place is the place nominated as the location of a delivery point if, in accordance with the criteria set out in subsection (6), another more suitable location exists.

Changing delivery points

(8) If:
  (a) the location of a delivery point has been determined by the ACMA in respect of a particular kind of telecommunications service and of an interception agency; and

(b) as a result of a material change in the circumstances of the carrier concerned, the location of that point becomes unsuitable;

the carrier:

(c) may nominate another place as the location of that delivery point in respect of that kind of telecommunications service and of that interception agency; and

(d) must inform the Communications Access Co-ordinator of the place so nominated.

Note: The nominated location becomes a delivery point: see the definition of ***delivery point*** in subsection 5(1).

(9) If:

(a) the location of a delivery point has been determined by the ACMA in respect of a particular kind of telecommunications service and of an interception agency; and

(b) as a result of a material change in the circumstances of the interception agency, the location of that point becomes unsuitable; and

(c) the interception agency, either directly or through the Communications Access Co-ordinator, requests the carrier to nominate another place as the location of that delivery point;

the carrier must:

(d) nominate another place as the location of that delivery point in respect of that kind of telecommunications service and of that interception agency; and

(e) inform the Communications Access Co-ordinator of the place nominated.

Note: The nominated location becomes a delivery point: see the definition of ***delivery point*** in subsection 5(1).

(10) Subsections (2) to (7) apply in relation to a nomination under subsection (8) or (9) as if it were a nomination under subsection (1).

Part 5-3—Interception capability

Division 1—Obligations

189 Minister may make determinations

(1) The Minister may, by legislative instrument, make determinations in relation to interception capabilities applicable to a specified kind of telecommunications service that involves, or will involve, the use of a telecommunications system.

(2) A determination:

(a) must specify an international standard or guidelines (the ***international standard***), or the relevant part of the international standard, on which the determination is based; and

(b) must provide for interception capability by adopting, applying or incorporating the whole or a part of the international standard, with only such modifications as are necessary to facilitate the application of the standard or the relevant part of the standard in Australia (including any transitional arrangement in relation to an existing kind of telecommunications service that might be required); and

(c) must be accompanied by a copy of the international standard or of the relevant part of the international standard.

(3) For the purposes of subsection (2), the international standard specified in a determination:

(a) must deal primarily with the requirements of interception agencies in relation to the interception of communications passing over a telecommunications network and related matters; and

(b) may be a part of an international agreement or arrangement or a proposed international agreement or arrangement.

Matters to be taken into account

(4) Before making a determination under subsection (1), the Minister must take into account:

(a) the interests of law enforcement and national security; and

(b) the objects of the *Telecommunications Act 1997*; and

(c) the privacy of the users of telecommunications systems.

(5) The Minister may take into account any other matter the Minister considers relevant.

190 Obligations of persons covered by a determination

(1) If a determination under section 189 applies to a particular kind of telecommunications service that involves, or will involve, the use of a telecommunications system, each carrier supplying that kind of service must comply with the determination.

Note: The definition of ***carrier*** in subsection 5(1) includes carriage service providers.

(2) Without limiting subsection (1), if a carrier is required to have interception capability in relation to a particular kind of telecommunications service under the determination, the carrier is required to ensure that the capability is developed, installed and maintained.

Note 1: A person may be exempted from the requirements of this section under a provision of Division 2.

Note 2: The cost of this capability is to be borne by the carriers: see Division 2 of Part 5-6.

191 Obligations of persons not covered by a determination in relation to a kind of telecommunications service

(1) Each carrier supplying a particular kind of telecommunications service that is not covered by any determination under section 189 but that involves, or will involve, the use of a telecommunications system must ensure that the kind of service or the system has the capability to:

(a) enable a communication passing over the system to be intercepted in accordance with an interception warrant; and

(b) transmit lawfully intercepted information to the delivery points applicable in respect of that kind of service.

Note: The definition of ***carrier*** in subsection 5(1) includes carriage service providers.

(2) Without limiting subsection (1), the obligation under that subsection includes the obligation to ensure that the capability is developed, installed and maintained.

Note 1: A person may be exempted from the requirements of this section under a provision of Division 2.

Note 2: The cost of this capability is to be borne by the carriers: see Division 2 of Part 5-6.

Division 2—Exemptions

192 The Communications Access Co-ordinator may grant exemptions

(1) The Communications Access Co-ordinator may exempt a specified person from all or any of the obligations imposed on the person under Division 1 in so far as those obligations relate to a specified kind of telecommunications service.

(2) The exemption must be in writing.

(3) The exemption may be:
  (a) unconditional; or
  (b) subject to such conditions as are specified in the exemption.

(4) An exemption given under subsection (1) is not a legislative instrument.

(5) If:
  (a) a person applies in writing to the Communications Access Co-ordinator for an exemption under subsection (1) from all the obligations, or from particular obligations, imposed on the person under Division 1 in so far as those obligations relate to a specified kind of telecommunications service; and
  (b) the Co-ordinator does not make, and communicate to the applicant, a decision granting, or refusing to grant, the exemption within 60 days after the day on which the Co-ordinator receives the application;

the Co-ordinator is taken, at the end of that period of 60 days, to have granted an exemption to the applicant from the obligations to which the application relates in so far as those obligations relate to that kind of telecommunications service.

(6) An exemption that is taken under subsection (5) to have been granted to a person who applied for an exemption under subsection (1) has effect only until the Communications Access

Co-ordinator makes, and communicates to the person, a decision on the application.

Matters to be taken into account

(7) Before giving an exemption under subsection (1), the Communications Access Co-ordinator must take into account:
  (a) the interests of law enforcement and national security; and
  (b) the objects of the *Telecommunications Act 1997*.

(8) The Communications Access Co-ordinator may take into account any other matter he or she considers relevant.

193 ACMA may grant exemptions for trial services

(1) The ACMA may exempt a specified person from all or any of the obligations imposed on the person under Division 1 in so far as those obligations relate to a kind of telecommunications service that is a trial service.

(2) The ACMA must not grant an exemption unless the ACMA, after consulting any interception agencies that the ACMA considers appropriate, is satisfied that the exemption is unlikely to create a risk to national security or law enforcement.

(3) The exemption must be in writing.

(4) The exemption may be:
  (a) unconditional; or
  (b) subject to such conditions as are specified in the exemption.

(5) An exemption given under subsection (1) is not a legislative instrument.

Part 5-4—Interception capability plans

194 Definitions

In this Part:

carriage service provider has the same meaning as in the *Telecommunications Act 1997*.

carrier has the same meaning as in the *Telecommunications Act 1997*.

nominated carriage service provider means a carriage service provider covered by a declaration in force under subsection 197(4).

195 Nature of an interception capability plan

(1) An interception capability plan (***IC plan***) of a carrier or nominated carriage service provider is a written instrument that complies with subsections (2) and (3).

Matters to be included in the instrument

(2) The instrument must set out:

(a) a statement of the policies of the carrier or provider in relation to interception generally and of its strategies for compliance with its legal obligation to provide interception capabilities in relation to a particular kind of telecommunications service that involves, or will involve, the use of a telecommunications system; and

(b) a statement of the compliance by the carrier or provider with that legal obligation; and

(c) a statement of any relevant developments in the business of the carrier or provider that are proposed within the period of 5 years from the start of the plan and that, if implemented, are likely to affect those interception capabilities; and

(d) a statement of the locations at which communications passing over a telecommunications system are intercepted or proposed to be intercepted by the carrier or provider; and

(e) a list of employees of the carrier or provider with responsibility for interception and other related matters; and

(f) the matters determined by the Minister under subsection (4).

Approval of instrument

(3) The instrument must be approved by the chief executive officer (however described) of the carrier or provider or by a person authorised in writing by that officer for the purposes of this subsection to approve the instrument.

Ministerial determination

(4) The Minister may, by legislative instrument, determine matters for the purposes of paragraph (2)(f).

(5) The Minister must consult the ACMA before making a determination under subsection (4).

IC plans are not legislative instruments

(6) An instrument made under subsection (1) is not a legislative instrument.

196 Time for giving IC plans by carriers

(1) A carrier must give an IC plan to the Communications Access Co-ordinator by:

(a) each 1 July; or

(b) if the Co-ordinator agrees to a later day instead of a particular 1 July—that later day.

Note: If the business plans of the carrier change, the carrier may be required to give the Co-ordinator another IC plan under section 201.

(2) The Communications Access Co-ordinator must inform the ACMA of any agreement under paragraph (1)(b).

Further rule for future carriers

(3) If the carrier became a carrier on a day (the ***start day***) after the commencement of this section, the carrier must also give an IC plan to the Communications Access Co-ordinator within 90 days after the start day.

197 Time for giving IC plans by nominated carriage service providers

(1) A nominated carriage service provider must give an IC plan to the Communications Access Co-ordinator by:

(a) each 1 July; or

(b) if the Co-ordinator agrees to a later day instead of a particular 1 July—that later day.

Note: If the business plans of the nominated carriage service provider change, the provider may be required to give the Co-ordinator another IC plan under section 201.

(2) The Communications Access Co-ordinator must inform the ACMA of any agreement under paragraph (1)(b).

Further rule for future nominated carriage service providers

(3) If the carriage service provider became a nominated carriage service provider on a day (the ***start day***) after the commencement of this section, the provider must also give an IC plan to the Communications Access Co-ordinator within 90 days after the start day.

Ministerial declaration

(4) For the purposes of this Part, the Minister may, by writing, declare a carriage service provider to be a nominated carriage service provider.

(5) A declaration made under subsection (4) is not a legislative instrument.

198 Consideration of IC plans

(1) If a carrier or a nominated carriage service provider gives the Communications Access Co-ordinator an IC plan under section 196, 197 or 201, or an amended IC plan under this section, the Co-ordinator must, within 60 days of receiving the plan:

(a) approve the plan and notify the carrier or provider of the approval; or

(b) give the plan back to the carrier or provider with a written request for the carrier or provider to give the Co-ordinator an amended IC plan to take account of specified matters.

Consultation with interception agencies and the ACMA

(2) As soon as practicable after receiving an IC plan (the ***original plan***) under section 196, 197 or 201, the Communications Access Co-ordinator must:

(a) give a copy of the plan to:

(i) the interception agencies that, in the opinion of the Co-ordinator, are likely to be interested in the plan; and

(ii) the ACMA; and

(b) invite each such interception agency to provide comments on the plan to the Co-ordinator.

Request for amendment of original plan

(3) If:

(a) the Communications Access Co-ordinator receives a comment from an interception agency requesting an amendment of the original plan; and

(b) the Co-ordinator considers the request to be a reasonable one;

the Co-ordinator must:

(c) give the carrier or provider a copy of the comment or a summary of the comment; and

(d) request that the carrier or provider respond to the comment or summary within the period (the ***response period***) of 30 days of receiving the comment or summary.

Response to request for amendment of original plan

(4) The carrier or provider must respond to a request for an amendment of the original plan either:

(a) by indicating its acceptance of the request, by amending the original plan appropriately and by giving the amended plan to the Communications Access Co-ordinator within the response period; or

(b) by indicating that it does not accept the request and providing its reasons for that non-acceptance.

The ACMA's role

(5) If the carrier or provider indicates that it does not accept a request for an amendment of the original plan, the Communications Access Co-ordinator must:

(a) refer the request and the carrier's or provider's response to the ACMA; and

(b) request the ACMA to determine whether any amendment of the original plan is required.

(6) The ACMA must then:

(a) determine in writing that no amendment of the original plan is required in response to the request for the amendment; or

(b) if, in the opinion of the ACMA:

(i) the request for the amendment is a reasonable one; and

(ii) the carrier's or provider's response to the request for the amendment is not reasonable;

determine in writing that the original plan should be amended in a specified manner and give a copy of the determination to the carrier or provider.

Amendment of original plan

(7) On receipt of a determination under paragraph (6)(b), the carrier or provider must:

(a) amend the original plan to take account of that determination; and

(b) give the amended plan to the Communications Access Co-ordinator.

ACMA determination not a legislative instrument

(8) A determination made under subsection (6) is not a legislative instrument.

199 Commencement of IC plans

An IC plan of a carrier or nominated carriage service provider:

(a) comes into force on the day the carrier or provider is notified by the Communications Access Co-ordinator that the plan has been approved; and

(b) continues in force until the day the carrier or provider is notified by the Co-ordinator that another IC plan of the carrier or provider has been approved.

200 Compliance with IC plans

During the period that an IC plan of a carrier or nominated carriage service provider is in force, the carrier or provider must ensure that its business activities are consistent with the plan.

201 Consequences of changed business plans

(1) If, because of changes to the business plans of a carrier or nominated carriage service provider, an IC plan given by that carrier or provider ceases, during the period before another such IC plan is due to be given, to constitute an adequate IC plan of that carrier or provider, the carrier or provider must:

(a) prepare a new IC plan having regard to those changed business plans; and

(b) give the new IC plan to the Communications Access Co-ordinator as soon as practicable.

Note: The new IC plan is subject to consideration in accordance with section 198.

(2) Subsection (1) applies only if the change in business plans has, or is likely to have, a material adverse effect on the ability of the carrier or provider to comply with its obligations under Part 5-3.

202 Confidential treatment of IC plans

Once the Communications Access Co-ordinator, the ACMA or an interception agency receives an IC plan of a carrier or nominated carriage service provider, the Co-ordinator, the ACMA or the interception agency:

(a) must treat the plan as confidential; and

(b) must ensure that it is not disclosed to any person or body not referred to in this section without the written permission of the carrier or provider.

Part 5-5—Delivery capability

203 Communications Access Co-ordinator may make determinations

(1) The Communications Access Co-ordinator may, by writing, make determinations in relation to delivery capabilities applicable in relation to:

(a) a specified kind of telecommunications service that involves, or will involve, the use of a telecommunications system and that is supplied by one or more specified carriers; and

(b) one or more specified interception agencies.

Note 1: The definition of ***carrier*** in subsection 5(1) includes carriage service providers.

Note 2: For specification by class, see subsection 46(3) of the *Acts Interpretation Act 1901*.

Note 3: A determination may make different provision with respect to different matters or different classes of matters (see subsection 33(3A) of the *Acts Interpretation Act 1901*).

(2) A determination under subsection (1) must relate to all or any of the following:

(a) the format in which lawfully intercepted information is to be delivered to an interception agency from the delivery point in respect of a kind of telecommunications service and of that interception agency;

(b) the place to which, and manner in which, that information is to be delivered;

(c) any ancillary information that should accompany that information.

(3) The Communications Access Co-ordinator must consult the ACMA before making a determination under subsection (1).

(4) A determination made under subsection (1) is not a legislative instrument.

204 Obligations of persons covered by a determination

(1) If a determination under section 203 applies:

(a) to a particular kind of telecommunications service that involves, or will involve, the use of a telecommunications system; and

(b) to a carrier;

the carrier must comply with the determination.

Note: The definition of ***carrier*** in subsection 5(1) includes carriage service providers.

(2) Without limiting subsection (1), if a carrier is required to have delivery capability in relation to a particular kind of telecommunications service under the determination, the carrier is required to ensure that the capability is developed, installed and maintained.

Note: The cost of this capability is to be borne by the interception agencies: see Division 3 of Part 5-6.

205 Obligations of persons not covered by a determination in relation to a kind of telecommunications service

(1) Each carrier supplying a particular kind of telecommunications service that is not covered by any determination under section 203 but that involves, or will involve, the use of a telecommunications system must ensure that the kind of service or the system has a delivery capability.

Note: The definition of ***carrier*** in subsection 5(1) includes carriage service providers.

(2) Without limiting subsection (1), the obligation under that subsection includes the obligation to ensure that the capability is developed, installed and maintained.

Note: The cost of this capability is to be borne by the interception agencies: see Division 3 of Part 5-6.

Part 5-6—Allocation of costs

Division 1—Outline of Part

206 Outline of Part

(1) Division 2 provides that the cost of developing, installing and maintaining an interception capability imposed on a carrier under Part 5-3 is to be borne by the carrier.

(2) Division 3 provides that the cost of developing, installing and maintaining a delivery capability imposed on a carrier under Part 5-5 is to be borne by the interception agencies.

Note: This Part does not deal with the allocation of costs in relation to carriers complying with authorisations under Division 3 or 4 of Part 4-1. Section 314 of the *Telecommunications Act 1997* deals with this matter.

Division 2—Interception capability

207 Costs to be borne by the carriers

The capital and ongoing costs of developing, installing and maintaining a capability imposed on a carrier under section 190 or 191 in respect of a particular kind of telecommunications service are to be borne by the carrier.

Note: The definition of ***carrier*** in subsection 5(1) includes carriage service providers.

Division 3—Delivery capability

208 Costs to be borne by the interception agencies

The capital and ongoing costs, worked out in accordance with section 209, of developing, installing and maintaining a delivery capability imposed on a carrier under Part 5-5 in respect of a particular kind of telecommunications service are to be borne by the interception agency concerned.

Note: The definition of ***carrier*** in subsection 5(1) includes carriage service providers.

209 Working out costs of delivery capabilities

(1) Each carrier who is obliged to ensure the development, installation and maintenance of a delivery capability must ensure that the capability is developed, installed and maintained on such terms and conditions:

(a) as are agreed in writing between the carrier and the interception agency concerned; or

(b) in the absence of such an agreement—as are determined in writing by the ACMA.

(2) The terms and conditions on which a carrier is to provide a delivery capability must be consistent with the following principles:

(a) the principle that the most cost effective means of ensuring the development, installation and maintenance of that capability is employed;

(b) the principle that the carrier is to incur the costs (whether of a capital nature or otherwise) relating to the development, installation and maintenance of that capability;

(c) the principle that the carrier may, over time, recover from an interception agency such of those costs as are required, under section 208, to be borne by that interception agency.

(3) Nothing in subsection (2) prevents a carrier from entering into an agreement with more than one interception agency.

(4) The agreement should also provide that if the working out of the costs to a particular interception agency of developing, installing and maintaining a delivery capability is the subject of a disagreement between the carrier and that interception agency:

(a) the interception agency may request the ACMA to arbitrate the matter; and

(b) if it does so, those costs are to be as determined by the ACMA.

(5) The regulations may make provision in relation to the conduct of an arbitration by the ACMA under this section.

(6) The existence of a cost dispute in relation to a delivery capability does not affect the obligations of the carrier in respect of that capability while that dispute is being resolved.

(7) If, as a result of the arbitration of a cost dispute between the carrier and an interception agency, the ACMA concludes that a lesser rate of charge would have been available, the carrier:

(a) must allow the interception agency credit for any costs already charged to the extent that they were worked out at a rate that exceeds that lesser rate; and

(b) must adjust its means of working out future costs;

to take account of that conclusion.

(8) For the purposes of this section, any reference in this section to terms and conditions agreed between a carrier and an interception agency includes a reference to terms and conditions agreed between the carrier and:

(a) in the case of an interception agency of a State—the State, on behalf of the interception agency; and

(b) in the case of an interception agency of the Commonwealth—the Commonwealth, on behalf of the interception agency.

(9) A determination made under paragraph (1)(b) is not a legislative instrument.

210 Examination of lower cost options

(1) In undertaking an arbitration under section 209, the ACMA may on its own initiative or at the request of an interception agency, by notice in writing given to a carrier, require the carrier:
   (a) to examine, at the expense of the carrier, the possibility of a lower cost option than the one designated by the carrier for providing a delivery capability; and
   (b) to report to the ACMA, within a period specified in the notice, on the results of that examination.

(2) If a carrier receives a notice under subsection (1), the carrier must, within the period specified in the notice:
   (a) carry out the examination concerned; and
   (b) report in writing to the ACMA on the results of the examination.

(3) A notice given under subsection (1) is not a legislative instrument.

211 ACMA may require independent audit of costs

(1) In undertaking an arbitration under section 209, the ACMA may, by notice in writing, require a carrier to arrange for an audit of the costs claimed to have been incurred by the carrier in relation to the provision to an interception agency of a delivery capability.

(2) Subject to subsection (3), the audit is to be carried out by an auditor selected by the carrier and approved by the ACMA.

(3) If the auditor selected by a carrier is not approved by the ACMA, the ACMA may require that the audit be carried out by an auditor selected by the ACMA or by the ACMA itself.

(4) Unless the audit is carried out by the ACMA itself, the ACMA may, in the notice requiring the audit, specify the period within which the auditor is to report to the ACMA.

(5) If a carrier receives a notice under this section, the carrier:

(a) must co-operate in full with the person or body carrying out the audit; and

(b) must bear the costs of the audit.

(6) A notice given under this section is not a legislative instrument.

Part 2—Consequential amendments

Australian Communications and Media Authority Act 2005

13 After subparagraph 8(1)(j)(iv)

Insert:

(iva) Chapter 4 or 5 of the *Telecommunications (Interception and Access) Act 1979*; or

Criminal Code Act 1995

14 Paragraph 476.5(2A)(b) of the *Criminal Code*

Omit "section 283 of the *Telecommunications Act 1997*", substitute "Division 3 of Part 4-1 of the *Telecommunications (Interception and Access) Act 1979*".

Intelligence Services Act 2001

15 Paragraph 14(2A)(b)

Omit "section 283 of the *Telecommunications Act 1997*", substitute "Division 3 of Part 4-1 of the *Telecommunications (Interception and Access) Act 1979*".

Telecommunications Act 1997

16 Section 5

Omit:

> • A carrier or carriage service provider may be required to have an ***interception capability***.

17 Section 6 (table item 18)

Repeal the item.

18 Section 7 (after paragraph (b) of the definition of *ACMA's telecommunications powers*)

Insert:

(ba) Chapter 4 or 5 of the *Telecommunications (Interception and Access) Act 1979*; or

19 Section 7 (definition of *agency*)

Repeal the definition.

20 Section 7 (definition of *agency co-ordinator*)

Repeal the definition.

21 Section 7

Insert:

Communications Access Co-ordinator has the meaning given by section 6R of the *Telecommunications (Interception and Access) Act 1979*.

22 Section 7 (definition of *IC plan*)

Repeal the definition.

23 Section 7 (definition of *interception related information*)

Repeal the definition.

24 Section 7A

Repeal the section.

25 Subsections 53A(1) and (2)

Omit "agency co-ordinator", substitute "Communications Access Co-ordinator".

Note: The heading to section 53A is altered by omitting "**agency co-ordinator**" and substituting "**Communications Access Co-ordinator**".

26 Section 56A

Omit "agency co-ordinator" (wherever occurring), substitute "Communications Access Co-ordinator".

Note: The heading to section 56A is altered by omitting "**agency co-ordinator**" and substituting "**Communications Access Co-ordinator**".

27 Subsection 59(8) (note after the definition of *application day*)

Omit "agency co-ordinator", substitute "Communications Access Co-ordinator".

28 Subsection 276(3) (at the end of note 1)

Add "of this Part and in Chapter 4 of the *Telecommunications (Interception and Access) Act 1979*".

29 Subsection 277(3) (at the end of note 1)

Add "of this Part and in Chapter 4 of the *Telecommunications (Interception and Access) Act 1979*".

30 Subsection 278(3) (at the end of note 1)

Add "of this Part and in Chapter 4 of the *Telecommunications (Interception and Access) Act 1979*".

31 Subsection 280(2) (definition of *enforcement agency*)

Omit "section 282", substitute "the *Telecommunications (Interception and Access) Act 1979*".

32 Sections 282 and 283

Repeal the sections.

33 At the end of section 294

Add "or in Divisions 3 to 5 of Part 4-1 of the *Telecommunications (Interception and Access) Act 1979*".

Note: The heading to section 294 is replaced by the heading "**Effect of this Subdivision**".

34 Subsection 295(1)

After "this Division", insert "or in Chapter 4 of the *Telecommunications (Interception and Access) Act 1979*".

35 At the end of subsection 295(2)

Add "or in Chapter 4 of the *Telecommunications (Interception and Access) Act 1979*".

36 Section 298

Repeal the section.

37 Section 305

Repeal the section, substitute:

305 Authorisations under the *Telecommunications (Interception and Access) Act 1979*

(1) This section applies if:

(a) a carrier, carriage service provider or number-database operator; or

(b) an associate of a carrier, carriage service provider or number-database operator;

is notified of an authorisation made under Division 4 of Part 4-1 of the *Telecommunications (Interception and Access) Act 1979*.

Note: Section 184 of the *Telecommunications (Interception and Access) Act 1979* deals with notification of such authorisations.

(2) The carrier, carriage service provider or number-database operator must retain the notification for 3 years.

38 Paragraph 306(1)(b)

Repeal the paragraph, substitute:

(b) the disclosure is authorised by:

(i) a provision of Division 3 (other than section 279, 285, 290 or 291); or

(ii) section 177, 178 or 179 or subsection 180(3) of the *Telecommunications (Interception and Access) Act 1979*.

Note: The heading to section 306 is altered by adding at the end "**—general**".

39 Paragraph 306(5)(d)

Repeal the paragraph, substitute:

(d) if the disclosure is made on the grounds of an authorisation under the *Telecommunications (Interception and Access) Act 1979*:

(i) the name of the person who made the authorisation; and

(ii) the date of the making of the authorisation; and

40 Paragraph 306(5)(e)

Omit "agency" (wherever occurring), substitute "body".

41 After section 306

Insert:

306A Record of disclosures—prospective authorisation under the *Telecommunications (Interception and Access) Act 1979*

(1) This section applies if:
  (a) an eligible person or an eligible number-database person discloses information or a document; and
  (b) the disclosure or disclosures are authorised by an authorisation under section 180 of the *Telecommunications (Interception and Access) Act 1979* (in so far as the authorisation is of a kind referred to in subsection 180(2) of that Act).

(2) If the person is a carrier, carriage service provider or number-database operator, the carrier, provider or operator must:
  (a) make a record of the disclosure or disclosures as soon as practicable after the day on which the authorisation ceases to be in force and, in any event, within 5 days after that day; and
  (b) retain that record for 3 years.

(3) If the person is an associate of a carrier, carriage service provider or number-database operator, the person must:
  (a) make a record of the disclosure or disclosures as soon as practicable after the day on which the authorisation ceases to be in force and, in any event, within 5 days after that day; and
  (b) give a copy of that record to the carrier, provider or operator within 5 days after the making of the record.

(4) If a copy of a record is given to a carrier, carriage service provider or number-database operator under subsection (3), the carrier, provider or operator must retain that copy for 3 years.

(5) A record made under subsection (2) or (3) must set out:
  (a) the name of the person or persons who made the disclosure or disclosures; and
  (b) one of the following:
    (i) if only 1 disclosure is made because of the authorisation—the date of the disclosure;

(ii) if more than 1 disclosure is made because of the authorisation—the date of the first disclosure and the date of the last disclosure; and

(c) a statement of the grounds for the disclosure or disclosures; and

(d) the name of the person who made the authorisation and the date of the making of the authorisation.

(6) A record, or a copy of a record, may be made, given or retained under this section:

(a) in written form; or

(b) in electronic form.

(7) A person who contravenes this section commits an offence punishable on conviction by a fine not exceeding 300 penalty units.

Note: See also sections 4AA and 4B of the *Crimes Act 1914*.

42 Subsection 307(1)

After "section 306", insert "or 306A".

43 Subparagraphs 308(1)(b)(i) and (ii)

After "section 306", insert "or 306A".

44 Paragraph 309(2)(a)

After "section 306", insert "or 306A".

45 Paragraph 309(2)(b)

Omit "Division 3 (which deals", substitute "Division 3 of this Part or Chapter 4 of the *Telecommunications (Interception and Access) Act 1979* (which deal".

46 Subsections 313(7) and (8)

Repeal the subsections, substitute:

(7) A reference in this section to giving help includes a reference to giving help by way of:

(a) the provision of interception services, including services in executing an interception warrant under the *Telecommunications (Interception and Access) Act 1979*; or

(b) giving effect to a stored communications warrant under that Act; or

(c) providing relevant information about:

(i) any communication that is lawfully intercepted under such an interception warrant; or

(ii) any communication that is lawfully accessed under such a stored communications warrant; or

(d) giving effect to authorisations under Division 3 or 4 of Part 4-1 of that Act; or

(e) disclosing information or a document in accordance with section 280 of this Act.

Note: Additional obligations concerning interception capability and delivery capability are, or may be, imposed on a carrier or carriage service provider under Chapter 5 of the *Telecommunications (Interception and Access) Act 1979*.

47 Subsection 314(2)

Omit "(except to the extent that the compliance involves costs that are, in accordance with the principles set out in subsection (3A), required to be borne by the person)".

48 Subsection 314(3)

Omit "Subject to subsection (3A), the", substitute "The".

49 Subsections 314(3A) and (3B)

Repeal the subsections.

50 At the end of section 314

Add:

(8) This section does not apply in relation to the obligation of carriers or carriage service providers under Part 5-3 or 5-5 of the *Telecommunications (Interception and Access) Act 1979* (about interception capability and delivery capability).

Note: Part 5-6 of the *Telecommunications (Interception and Access) Act 1979* contains provisions about the allocation of costs in relation to interception capability and delivery capability.

51 Section 314A

Repeal the section.

52 Part 15

Repeal the Part.

53 Subclause 1(2) of Schedule 1 (at the end of the definition of *this Act*)

Add "and Chapter 5 of the *Telecommunications (Interception and Access) Act 1979*".

54 Subclause 1(2) of Schedule 2 (at the end of the definition of *this Act*)

Add "and Chapter 5 of the *Telecommunications (Interception and Access) Act 1979*".

Telecommunications (Interception and Access) Act 1979

55 Chapter 5 (heading)

Repeal the heading, substitute:

Chapter 6—Regulations

56 Part 5-1 (heading)

Repeal the heading, substitute:

Part 6-1—Regulations

Part 3—Application, saving and transitional provisions

57 Definitions

In this Part:

ACMA means the Australian Communications and Media Authority.

TIA Act means the *Telecommunications (Interception and Access) Act 1979*.

58 Transitional—certificates of the Organisation

If:

(a) a certificate was in force under paragraph 283(2)(b) of the *Telecommunications Act 1997* immediately before the commencement of this item; and

(b) before that commencement, a copy of the certificate was given to the person from whom the disclosure was sought; and

(c) before that commencement, no disclosure had been made as permitted by the certificate;

then the certificate has effect after that commencement as if it were an authorisation in force under subsection 175(2) of the TIA Act that authorised the disclosure of information or documents of a kind covered by the certificate that came into existence before that commencement.

59 Transitional—certificates of enforcement agencies

Enforcement of the criminal law

(1) If:

(a) a certificate was in force under subsection 282(3) of the *Telecommunications Act 1997* immediately before the commencement of this item; and

(b) before that commencement, a copy of the certificate was given in accordance with subsection 305(2) or (3) of that Act; and

(c) before that commencement, no disclosure had been made as permitted by the certificate;

then the certificate has effect after that commencement as if it were an authorisation in force under subsection 178(2) of the TIA Act that authorised the disclosure of information or documents of a kind covered by the certificate that came into existence before that commencement.

Enforcement of a law imposing a pecuniary penalty or protection of the public revenue

(2) If:

(a) a certificate was in force under subsection 282(4) or (5) of the *Telecommunications Act 1997* immediately before the commencement of this item; and

(b) before that commencement, a copy of the certificate was given in accordance with subsection 305(2) or (3) of that Act; and

(c) before that commencement, no disclosure had been made as permitted by the certificate;

then the certificate has effect after that commencement as if it were an authorisation in force under subsection 179(2) of the TIA Act that authorised the disclosure of information or documents of a kind covered by the certificate that came into existence before that commencement.

Part 4-2 of the TIA Act does not apply

(3) Part 4-2 of the TIA Act does not apply to an authorisation referred to in this item.

60 Saving—secondary disclosure/use offences

Despite the repeal of section 298 of the *Telecommunications Act 1997* made by this Act, that section continues to apply after the commencement of this item in relation to disclosures made before or after that commencement as if that repeal had not been made.

61 Saving—record keeping

(1) Despite the amendment made by item 37 of this Schedule, section 305 of the *Telecommunications Act 1997* (as in force immediately before the commencement of that item) continues to apply after that commencement in relation to copies of certificates given before that commencement.

(2) Despite the amendment made by item 39 of this Schedule, paragraph 306(5)(d) of the *Telecommunications Act 1997* (as in force immediately before the commencement of that item) continues to apply after that commencement in relation to a disclosure made before that commencement on the grounds of a certificate under subsection 282(3), (4) or (5) of the *Telecommunications Act 1997*.

(3) For the purposes of section 306 of the *Telecommunications Act 1997*, if a disclosure is made because of an authorisation referred to in item 59 of this Part, paragraph 306(5)(d) of the *Telecommunications Act 1997* applies as if:

(a) the person who made the authorisation was the same person who issued the corresponding certificate under the *Telecommunications Act 1997*; and

(b) the authorisation was made on the day of commencement of this item.

62 Transitional—applications for carrier licences

If:

(a) an application was made under section 52 of the *Telecommunications Act 1997* before the commencement of this item; and

(b) the application had not been decided by the ACMA immediately before that commencement;

sections 53A and 56A of that Act apply after that commencement as if a reference to the Communications Access Co-ordinator included a reference to the agency co-ordinator (within the meaning of that Act immediately before that commencement).

63 Transitional—delivery points

(1) This item applies in relation to a delivery point (the ***old point***) in force, immediately before the commencement of this item, in respect of a carriage service of a carrier or carriage service provider and of an agency under section 314A of the *Telecommunications Act 1997*.

(2) At the commencement of this item:

(a) the old point is taken to be a delivery point (the ***new point***) in force under section 188 of the TIA Act in respect of the equivalent kind of telecommunications service of that carrier

or carriage service provider and of the equivalent interception agency; and

(b) if the old point was one determined by the ACMA, section 188 of the TIA Act applies as if the new point was one determined by the ACMA.

Note: Subsections 188(8) to (10) of the TIA Act set out the process for changing delivery points determined by the ACMA.

(3) If:

(a) before the commencement of this item:

(i) a notification of a disagreement was made under subsection 314A(2) of the *Telecommunications Act 1997*; or

(ii) a nomination was made under paragraph 314A(8)(c) of the *Telecommunications Act 1997*; or

(iii) a request was made under paragraph 314A(9)(c) of the *Telecommunications Act 1997*; and

(b) immediately before the commencement of this item, the procedures set out in section 314A of that Act for dealing with that disagreement, nomination or request had not ended;

then:

(c) despite the repeal of that section made by this Act, that section continues to apply after that commencement in relation to that disagreement, nomination or request as if the repeal had not been made; and

(d) a delivery point (the ***transitional point***) nominated or determined, after that commencement, under that section in respect of a carriage service of a carrier or carriage service provider and of an agency becomes a delivery point (the ***translated point***) under section 188 of the TIA Act in respect of the equivalent kind of telecommunications service of that carrier or provider and of the equivalent interception agency; and

(e) if the transitional point was one determined by the ACMA, section 188 of the TIA Act applies as if the translated point was one determined by the ACMA.

64 Transitional—exemptions from interception capability

Agency co-ordinator exemptions

(1) An exemption in force under subsection 326(1) of the *Telecommunications Act 1997* immediately before the commencement of this item in relation to a carriage service has effect after that commencement as if it were an exemption in force under subsection 192(1) of the TIA Act in relation to the equivalent kind of telecommunications service.

(2) If:

(a) an application was made under section 326 of the *Telecommunications Act 1997* before the commencement of this item in relation to a carriage service; and

(b) the application had not been decided (including because of the operation of subsection 326(4) of that Act) immediately before the commencement of this item;

then:

(c) the application has affect at the commencement of this item as if it had been made under section 192 of the TIA Act; and

(d) for the purposes of the Communications Access Co-ordinator deciding it, the Co-ordinator is taken to have received it on the day it was received under the *Telecommunications Act 1997*.

ACMA exemptions

(3) An exemption in force under subsection 327(1) of the *Telecommunications Act 1997* immediately before the commencement of this item in relation to a carriage service has effect after that commencement as if it were an exemption in force under subsection 193(1) of the TIA Act in relation to the equivalent kind of telecommunications service.

65 Transitional—nominated carriage service providers

A declaration in force under subsection 331(3) of the *Telecommunications Act 1997* immediately before the commencement of this item has effect after that commencement as if it were a declaration in force under subsection 197(4) of the TIA Act.

66 Transitional—IC plans

(1) An IC plan in force under Division 3 of Part 15 of the *Telecommunications Act 1997* immediately before the commencement of this item has effect after that commencement as if it were an IC plan in force under Part 5-4 of the TIA Act.

(2) If:

(a) before the commencement of this item, an IC plan was lodged under Division 3 of Part 15 of the *Telecommunications Act 1997*; and

(b) immediately before the commencement of this item, the procedures set out in section 332C of that Act for dealing with that plan had not ended;

then:

(c) at the commencement of this item, the plan is taken to have been given under Part 5-4 of the TIA Act; and

(d) the plan must be dealt with in accordance with section 198 of the TIA Act.

(3) For the purposes of paragraph (2)(d), a thing:

(a) that is required to occur under section 198 of the TIA Act in relation to the plan; and

(b) that already occurred under section 332C of the *Telecommunications Act 1997* in relation to the plan;

is taken to have already occurred under section 198 of the TIA Act in relation to the plan.

67 Section 8 of the *Acts Interpretation Act 1901*

This Part does not limit the operation of section 8 of the *Acts Interpretation Act 1901* in relation to the amendments or repeals made by this Schedule.

68 Transitional regulations

The Governor-General may make regulations prescribing matters of a transitional nature (including prescribing any saving or application provisions) relating to the amendments or repeals made by this Schedule.

Schedule 2—Other amendments

Part 1—Amendments

Telecommunications (Interception) Amendment Act 2006

1 Item 8 of Schedule 5

Omit "**(c)**", substitute "**(d)**".

Note: This item corrects a misdescription of text in an amending item.

Telecommunications (Interception and Access) Act 1979

2 Subsection 5(1) (subparagraphs (d)(ii), (e)(ii) and (g)(iii) of the definition of *certifying officer*)

Omit "*Public Sector Management Act 1988*", substitute "*Public Sector Employment and Management Act 2002*".

3 Subsection 5(1)

Insert:

security authority means an authority of the Commonwealth that has functions primarily relating to:

(a) security; or

(b) collection of foreign intelligence; or

(c) the defence of Australia; or

(d) the conduct of the Commonwealth's international affairs.

4 After subsection 5(4A)

Insert:

(4B) A reference in this Act to an employee of a security authority includes a reference to a person who is engaged by the security authority or whose services are made available to the security authority.

5 After paragraph 5B(1)(b)

Insert:

(ba) a proceeding under the *Spam Act 2003*; or

6 Subparagraphs 5D(2)(b)(viii) and (ix)

Repeal the subparagraphs.

7 After subsection 5D(3A)

Insert:

Offences relating to child pornography

(3B) An offence is also a ***serious offence*** if the particular conduct constituting the offence involved, involves or would involve, as the case requires:

(a) the production, publication, possession, supply or sale of, or other dealing in, child pornography; or

(b) consenting to or procuring the employment of a child, or employing a child, in connection with child pornography.

8 Paragraph 5D(4)(c)

Omit "section 122 of the **Confiscation Act 1997**", substitute "section 194, 195 or 195A of the **Crimes Act 1958**".

9 Paragraph 5D(4)(f)

Omit "section 10b of the *Crimes (Confiscation of Profits) Act, 1986*", substitute "section 138 of the *Criminal Law Consolidation Act 1935*".

10 At the end of subsection 5D(4)

Add:

; (i) Division 3A of Part VII of Schedule I to the *Criminal Code Act* of the Northern Territory.

11 Subsection 5F(2)

Repeal the subsection, substitute:

(2) However, if a communication is sent from an address on a computer network operated by or on behalf of:

(a) a Commonwealth agency; or

(b) a security authority; or

(c) an eligible authority of a State;

the communication 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:

(d) any employee, member of staff or officer of the agency or authority responsible for operating, protecting or maintaining the network;

(e) any employee, member of staff or officer of the agency or authority responsible for enforcement of the professional standards (however described) of the agency or authority.

12 Subsection 5G(2)

Repeal the subsection, substitute:

(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:

(a) a Commonwealth agency; or

(b) a security authority; or

(c) an eligible authority of a State;

each of the following is also an ***intended recipient*** of the communication for the purposes of this Act:

(d) any employee, member of staff or officer of the agency or authority responsible for operating, protecting or maintaining the network;

(e) any employee, member of staff or officer of the agency or authority responsible for enforcement of the professional standards (however described) of the agency or authority.

13 At the end of paragraphs 7(2)(a), (aa), (ab) and (ac)

Add "or".

14 At the end of subsection 7(2)

Add:

; or (d) the interception of a communication under an authorisation under section 31A.

15 Subsection 9A(1A) (the subsection (1A) inserted by item 7 of Schedule 1 to the *Telecommunications (Interception) Amendment Act 2006*)

Renumber as subsection (1C).

16 After Part 2-3

Insert:

Part 2-4—Authorisation of interception for developing and testing interception capabilities

31 Applications for authorisation

(1) The head (however described) of a security authority that has functions that include activities relating to developing or testing technologies, or interception capabilities, or a person acting as that head, may request the Attorney-General to authorise, under section 31A, interception of communications passing over a telecommunications system by employees of the authority authorised under section 31B.

(2) The request:

(a) must be in writing; and

(b) must include details of the development or testing of technologies, or interception capabilities, in relation to which authorisation is sought; and

(c) must include details of the extent to which the development or testing would involve, or would be likely to involve, interception of communications passing over a telecommunications system; and

(d) must refer to the functions of the authority that the development or testing would support; and

(e) must state the grounds for seeking the authorisation; and

(f) must summarise the outcomes of any previous authorisations given to the authority under section 31A in relation to the technology or interception capability that is the subject of the application; and

(g) must nominate the period (not exceeding 6 months) for which the authorisation is sought to be in force.

31A Attorney-General may authorise interception for developing and testing interception capabilities

(1) Upon receiving the request, the Attorney-General may authorise interception of communications passing over a telecommunications system by employees of the security authority authorised under section 31B.

(2) The authorisation is subject to:

(a) a condition prohibiting:

(i) interception of communications passing over a telecommunications system except for the purposes of development or testing of technologies, or interception capabilities; or

(ii) communicating, using or recording such communications except for such purposes; and

(b) any other conditions specified in the authorisation.

(3) The authorisation must be in writing and must specify the period (not exceeding 6 months) for which it will have effect.

(4) The head (however described) of the security authority, or a person acting as that head, must ensure that a copy of the authorisation is kept by the authority and is available for inspection on request by the Minister who is responsible for the authority.

(5) An authorisation given under subsection (1) is not a legislative instrument.

31B Authorisation of employees of a security authority

(1) The following persons:

(a) the head (however described) of a security authority;

(b) an officer of the security authority covered by an approval in force under subsection (2);

may, by writing, authorise employees of the authority for the purposes of this Part.

(2) The head (however described) of a security authority may, by writing, approve an officer of the authority for the purposes of paragraph (1)(b).

31C Destruction of records

If:

(a) information, or a record, that was obtained, in the course of developing or testing technologies or interception capabilities, by interception of communications passing over a telecommunications system is in a security authority's possession; and

(b) the information or record is no longer required in relation to the development or testing;

the head (however described) of the security authority, or a person acting as that head, must cause the information or record to be destroyed as soon as practicable.

31D Reports to the Attorney-General

The head (however described) of a security authority, or a person acting as that head, must give to the Attorney-General, within 3 months after an authorisation under section 31A given to the authority ceases to have effect, a written report about:

(a) the outcome of the development or testing of technologies, or interception capabilities, in relation to which the authorisation was given; and

(b) the destruction of information or records under section 31C.

17 Subsection 61(1)

Repeal the subsection, substitute:

(1) The following:

(a) the Managing Director of a carrier;

(b) the secretary of a carrier;

(c) an employee of a carrier authorised in writing for the purposes of this paragraph by the Managing Director or the secretary of the carrier;

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.

18 Subsection 61(2)

After "secretary", insert ", or an employee,".

19 Paragraph 139(2)(a)

After "agency", insert "or by another enforcement agency".

20 After paragraph 139(4)(b)

Insert:

(ba) a proceeding under the *Spam Act 2003*; or

21 At the end of subsection 139(4)

Add:

; or (f) a police disciplinary proceeding.

Part 2—Application and transitional provisions

22 Application—exempt proceedings

The amendment made by item 5 of this Schedule applies in relation to proceedings instituted before or after the commencement of that item.

23 Application—serious offences

The amendment made by item 7 of this Schedule applies in relation to conduct engaged in before or after the commencement of that item.

24 Transitional—continuation of evidentiary certificates

A certificate in force immediately before the commencement of this item under subsection 61(1) of the *Telecommunications (Interception and Access) Act 1979* continues in force after that commencement as if it had been issued under that subsection after that commencement.

25 Application—permitted dealings with accessed information

The amendments made by items 20 and 21 of this Schedule apply in relation to proceedings instituted before or after the commencement of those items.

26 Transitional—issue of evidentiary certificates in relation to old warrants

Paragraph 61(4)(a) of the *Telecommunications (Interception and Access) Act 1979* applies as if a reference to a Part 2-5 warrant included a reference to a warrant issued under Part VI of that Act as in force before 13 June 2006.

[*Minister's second reading speech made in—*
House of Representatives on 14 June 2007
Senate on 16 August 2007]

(110/07)