2013-2014

The Parliament of the
Commonwealth of Australia

HOUSE OF REPRESENTATIVES

Presented and read a first time

Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014

No. , 2014

(Attorney-General)

A Bill for an Act to amend the *Telecommunications (Interception and Access) Act 1979*, and for related purposes

Contents

A Bill for an Act to amend the *Telecommunications (Interception and Access) Act 1979*, and for related purposes

The Parliament of Australia enacts:

1 Short title

This Act may be cited as the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2014*.

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**
Provisions	**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.	
2. Schedule 1, items 1 to 7	The day after the end of the period of 6 months beginning on the day this Act receives the Royal Assent.	
3. Schedule 1, items 8 to 11	The day this Act receives the Royal Assent.	
4. Schedules 2 and 3	The day after the end of the period of 6 months beginning on the day 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Note: This table relates only to the provisions of this Act as originally enacted.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 Schedules

Legislation that is specified in a Schedule to this Act is amended or repealed as set out in the applicable items in the Schedule concerned, and any other item in a Schedule to this Act has effect according to its terms.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

Part 1—Main amendments

Telecommunications (Interception and Access) Act 1979

1 After Part 5-1

Insert:

Part 5-1A—Data retention

Division 1—Obligation to keep information and documents

187A Service providers must keep certain information and documents

(1) A person (a ***service provider***) who operates a service to which this Part applies (a ***relevant service***) must keep, or cause to be kept, for the period specified in section 187C:

(a) information of a kind prescribed by the regulations; or

(b) documents containing information of that kind;

relating to any communication carried by means of the service.

Note 1: Subsection (3) sets out the services to which this Part applies.

Note 2: Section 187B removes some service providers from the scope of this obligation, either completely or in relation to some services they operate.

Note 3: Division 3 provides for exemptions from a service provider's obligations under this Part.

(2) The kinds of information prescribed for the purposes of paragraph (1)(a) must relate to one or more of the following matters:

(a) characteristics of any of the following:

(i) the subscriber of a relevant service;

(ii) an account relating to a relevant service;

(iii) a telecommunications device relating to a relevant service;

(iv) another relevant service relating to a relevant service;

(b) the source of a communication;

(c) the destination of a communication;

(d) the date, time and duration of a communication, or of its connection to a relevant service;

(e) the type of a communication, or a type of relevant service used in connection with a communication;

(f) the location of equipment, or a line, used in connection with a communication.

(3) This Part applies to a service if:

(a) it is a service for carrying communications, or enabling communications to be carried, by means of guided or unguided electromagnetic energy or both; and

(b) it is a service:

(i) operated by a carrier; or

(ii) operated by an internet service provider (within the meaning of Schedule 5 to the *Broadcasting Services Act 1992*); or

(iii) of a kind prescribed by the regulations; and

(c) the person operating the service owns or operates, in Australia, infrastructure that enables the provision of any of its relevant services;

but does not apply to a broadcasting service (within the meaning of the *Broadcasting Services Act 1992*).

(4) This section does not require a service provider to keep, or cause to be kept:

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

Note: This paragraph puts beyond doubt that service providers are not required to keep information about telecommunications content.

(b) information that:

(i) states an address to which a communication was sent on the internet, from a telecommunications device, using an internet access service provided by the service provider; and

(ii) was obtained by the service provider only as a result of providing the service; or

Note: This paragraph puts beyond doubt that service providers are not required to keep information about subscribers' web browsing history.

(c) information to the extent that it relates to a communication carried by means of another relevant service operated:

(i) by another service provider; and

(ii) using the relevant service;

or a document to the extent that the document contains such information; or

(d) information that the service provider is required to delete because of a determination made under section 99 of the *Telecommunications Act 1997*, or a document to the extent that the document contains such information; or

(e) information about the location of a telecommunications device that is not information used by the service provider in relation to the relevant service to which the device is connected.

(5) Without limiting subsection (1), for the purposes of this section:

(a) an attempt to send a communication by means of a relevant service is taken to be the sending of a communication by means of the service, if the attempt results in:

(i) a connection between the telecommunications device used in the attempt and another telecommunications device; or

(ii) an attempted connection between the telecommunications device used in the attempt and another telecommunications device; or

(iii) a conclusion being drawn, through the operation of the service, that a connection cannot be made between the telecommunications device used in the attempt and another telecommunications device; and

(b) an untariffed communication by means of a relevant service is taken to be a communication by means of the service.

(6) To avoid doubt, if information that subsection (1) requires a service provider to keep in relation to a communication is not created by the operation of a relevant service, subsection (1)

requires the service provider to use other means to create the information, or a document containing the information.

(7) For the purposes of paragraphs (2)(b), (c), (d) and (f) and regulations made for the purposes of those paragraphs, 2 or more communications that together constitute a single communications session are taken to be a single communication.

187B Certain service providers not covered by this Part

(1) Subsection 187A(1) does not apply to a service provider (other than a carrier that is not a carriage service provider) in relation to a relevant service that it operates if:

(a) the service:

(i) is provided only to a person's immediate circle (within the meaning of section 23 of the *Telecommunications Act 1997*); or

(ii) is provided only to places that, under section 36 of that Act, are all in the same area; and

(b) the service is not subject to a declaration under subsection (2) of this section.

(2) The Communications Access Co-ordinator may declare that subsection 187A(1) applies in relation to a relevant service that a service provider operates.

(3) In considering whether to make the declaration, the Communications Access Co-ordinator must have regard to:

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

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

(c) any other matter that the Communications Access Co-ordinator considers relevant.

(4) The declaration must be in writing.

(5) A declaration made under subsection (2) is not a legislative instrument.

187C Period for keeping information and documents

(1) The period for which a service provider must keep, or cause to be kept, information or a document under section 187A is:

(a) if the information is about, or the document contains information about, a matter of a kind described in paragraph 187A(2)(a)—the period:

(i) starting when the information or document came into existence; and

(ii) ending 2 years after the closure of the account to which the information or document relates; or

(b) otherwise—the period:

(i) starting when the information or document came into existence; and

(ii) ending 2 years after it came into existence.

(2) However, the regulations may prescribe that, in relation to a specified matter of a kind described in paragraph 187A(2)(a), the period under subsection (1) of this section is the period referred to in paragraph (1)(b) of this section.

(3) This section does not prevent a service provider from keeping information or a document for a period that is longer than the period provided under this section.

Note: Division 3 provides for reductions in periods specified under this section.

Division 2—Data retention implementation plans

187D Effect of data retention implementation plans

While there is in force a data retention implementation plan for a relevant service operated by a service provider:

(a) the service provider must comply with the plan in relation to communications carried by means of that service; but

(b) the service provider is not required to comply with subsection 187A(1) (or section 187C) in relation to those communications.

187E Applying for approval of data retention implementation plans

(1) A service provider may apply to the Communications Access Co-ordinator for approval of a data retention implementation plan for one or more relevant services operated by the service provider.

(2) The plan must specify, in relation to each such service:

(a) an explanation of the current practices for keeping information and documents that section 187A would require to be kept, if the plan were not in force; and

(b) details of the interim arrangements that the service provider proposes to be implemented, while the plan is in force, for keeping such information and documents (to the extent that the information and documents will not be kept in compliance with section 187A (and section 187C)); and

(c) the day by which the service provider will comply with section 187A (and section 187C) in relation to all such information and documents, except to the extent that any decisions under Division 3 apply.

(3) The day specified under paragraph (2)(c) must not be later than the day on which the plan would, if approved, cease to be in force under section 187H in relation to the service.

(4) The plan must also specify:

(a) any relevant services, operated by the service provider, that the plan does not cover; and

(b) the contact details of the officers or employees of the service provider in relation to the plan.

187F Approval of data retention implementation plans

(1) If, under section 187E, a service provider applies for approval of a data retention implementation plan, the Communications Access Co-ordinator must:

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

(b) give the plan back to the service provider with a written request for the service provider to amend the plan to take account of specified matters.

(2) Before making a decision under subsection (1), the Communications Access Co-ordinator must take into account:

(a) the desirability of achieving substantial compliance with section 187A (and section 187C) as soon as practicable; and

(b) the extent to which the plan would reduce the regulatory burden imposed on the service provider by this Part; and

(c) if, at the time the Co-ordinator receives the application, the service provider is contravening section 187A (or section 187C) in relation to one or more services covered by the application—the reasons for the contravention; and

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

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

(f) any other matter that the Co-ordinator considers relevant.

(3) If the Communications Access Co-ordinator does not, within 60 days after the day the Co-ordinator receives the application:

(a) make a decision on the application, and

(b) communicate to the applicant the decision on the application;

the Co-ordinator is taken, at the end of that period of 60 days, to have made the decision that the service provider applied for, and to have notified the service provider accordingly.

(4) A decision that is taken under subsection (3) to have been made in relation to a service provider that applied for the decision has effect only until the Communications Access Co-ordinator makes, and communicates to the service provider, a decision on the application.

187G Consultation with agencies and the ACMA

(1) As soon as practicable after receiving an application under section 187E to approve a data retention implementation plan (the ***original plan***), the Communications Access Co-ordinator must:

(a) give a copy of the plan to the enforcement agencies and security authorities that, in the opinion of the Co-ordinator, are likely to be interested in the plan; and

(b) invite each such enforcement agency or security authority to provide comments on the plan to the Co-ordinator.

The Co-ordinator may give a copy of the plan to the ACMA.

Request for amendment of original plan

(2) If:

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

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

the Co-ordinator:

(c) must request that the service provider make the amendment within 30 days (the ***response period***) after receiving the comment or summary; and

(d) may give the service provider a copy of the comment or a summary of the comment.

Response to request for amendment of original plan

(3) The service 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

(4) If the service 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 service provider's response to the ACMA; and

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

(5) 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 service 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 service provider.

Co-ordinator to approve amended plan or to refuse approval

(6) The Communications Access Co-ordinator must:

(a) if, on receipt of a determination under paragraph (5)(b), the service provider amends the original plan to take account of that determination and gives the amended plan to the Communications Access Co-ordinator—approve the plan as amended, and notify the service provider of the approval; or

(b) otherwise—refuse to approve the plan, and notify the service provider of the refusal.

ACMA determination not a legislative instrument

(7) A determination made under subsection (5) is not a legislative instrument.

187H When data retention implementation plans are in force

(1) A data retention implementation plan for a relevant service operated by a service provider:

(a) comes into force when the Communications Access Co-ordinator notifies the service provider of the approval of the plan; and

(b) ceases to be in force in relation to that service:

(i) if the service provider was operating the service at the commencement of this Part—at the end of the implementation phase for this Part; or

(ii) if the service provider was not operating the service at the commencement of this Part—at the end of the period of 18 months starting on the day the service provider started to operate the service after that commencement.

(2) The ***implementation phase*** for this Part is the end of the period of 18 months starting on the commencement of this Part.

187J Amending data retention implementation plans

(1) If a service provider's data retention implementation plan is in force, it may be amended only if:

(a) the service provider applies to the Communications Access Co-ordinator for approval of the amendment, and the Co-ordinator approves the amendment; or

(b) the Co-ordinator makes a request to the service provider for the amendment to be made, and the service provider agrees to the amendment.

(2) Section 187F applies in relation to approval of the amendment under paragraph (1)(a) as if the application for approval of the amendment were an application under section 187E for approval of a data retention implementation plan.

(3) An amendment of a data retention implementation plan:

(a) comes into force when:

(i) if paragraph (1)(a) applies—the Co-ordinator notifies the service provider of the approval of the amendment; or

(ii) if paragraph (1)(b) applies—the service provider notifies the Co-ordinator of the service provider's agreement to the amendment; but

(b) does not effect when the plan ceases to be in force under paragraph 187H(1)(b).

Division 3—Exemptions

187K The Communications Access Co-ordinator may grant exemptions or variations

Decision to exempt or vary

(1) The Communications Access Co-ordinator may:

(a) exempt a specified service provider from the obligations imposed on the service provider under this Part, either

generally or in so far as they relate to a specified kind of relevant service; or

(b) vary the obligations imposed on a specified service provider under this Part, either generally or in so far as they relate to a specified kind of relevant service; or

(c) vary, in relation to a specified service provider, a period specified in section 187C, either generally or in relation to information or documents that relate to a specified kind of relevant service.

A variation must not impose obligations that would exceed the obligations to which a service provider would otherwise be subject under sections 187A and 187C.

(2) The decision must be in writing.

(3) The decision may be:

(a) unconditional; or

(b) subject to such conditions as are specified in the exemption.

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

Effect of applying for exemption or variation

(5) If a service provider applies in writing to the Communications Access Co-ordinator for a particular decision under subsection (1) relating to the service provider:

(a) the Co-ordinator:

(i) must give a copy of the application to the enforcement agencies and security authorities that, in the opinion of the Co-ordinator, are likely to be interested in the application; and

(ii) may give a copy of the application to the ACMA; and

(b) if the Co-ordinator does not, within 60 days after the day the Co-ordinator receives the application:

(i) make a decision on the application, and

(ii) communicate to the applicant the decision on the application;

the Co-ordinator is taken, at the end of that period of 60 days, to have made the decision that the service provider applied for.

(6) A decision that is taken under paragraph (5)(b) to have been made in relation to a service provider that applied for the decision has effect only until the Communications Access Co-ordinator makes, and communicates to the service provider, a decision on the application.

Matters to be taken into account

(7) Before making a decision under subsection (1) in relation to a service provider, 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*; and

(c) the service provider's history of compliance with this Part; and

(d) the service provider's costs, or anticipated costs, of complying with this Part; and

(e) any alternative data retention arrangements that the service provider has identified.

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

Division 4—Miscellaneous

187L Confidentiality of applications

(1) If the Communications Access Co-ordinator receives a service provider's application under section 187E for approval of a data retention implementation plan, or application for a decision under subsection 187K(1), the Co-ordinator must:

(a) treat the application as confidential; and

(b) ensure that it is not disclosed to any other person or body (other than the ACMA, an enforcement agency or a security authority) without the written permission of the service provider.

(2) The ACMA, an enforcement agency or a security authority must, if it receives under paragraph 187G(1)(a) or 187K(5)(a) a copy of a service provider's application:

(a) treat the copy as confidential; and

(b) ensure that it is not disclosed to any other person or body without the written permission of the service provider.

187M Pecuniary penalties and infringement notices

Subsection 187A(1) and paragraph 187D(a) are civil penalty provisions for the purposes of the *Telecommunications Act 1997*.

Note: Parts 31 and 31B of the *Telecommunications Act 1997* provide for pecuniary penalties and infringement notices for contraventions of civil penalty provisions.

187N Review of operation of Part

(1) The Parliamentary Joint Committee on Intelligence and Security must review the operation of this Part as soon as practicable after the third anniversary of the end of the implementation phase for this Part.

(2) The Committee must give the Minister a written report of the review.

187P Annual reports

(1) The Minister must, as soon as practicable after each 30 June, cause to be prepared a written report on the operation of this Part during the year ending on that 30 June.

(2) A report under subsection (1) must be included in the report prepared under subsection 186(2) relating to the year ending on that 30 June.

(3) A report under subsection (1) must not be made in a manner that is likely to enable the identification of a person.

Part 2—Other amendments

Telecommunications Act 1997

2 Section 7 (at the end of the definition of *civil penalty provision*)

Add:

; or (c) a provision of the *Telecommunications (Interception and Access) Act 1979* that is declared by that Act to be a civil penalty provision for the purposes of this Act.

3 Subsection 105(5A)

Repeal the subsection, substitute:

(5A) The ACMA must monitor, and report each financial year to the Minister on:

(a) the operation of Part 14 and on the costs of compliance with the requirements of that Part; and

(b) without limiting paragraph (a), the costs of compliance with the requirements of Part 5-1A of the *Telecommunications (Interception and Access) Act 1979* (about data retention).

4 Subsection 314(8)

Omit "Part 5-3 or 5-5 of the *Telecommunications (Interception and Access) Act 1979* (about", substitute "Part 5-1A, 5-3 or 5-5 of the *Telecommunications (Interception and Access) Act 1979* (about data retention,".

Telecommunications (Interception and Access) Act 1979

5 Subsection 5(1)

Insert:

implementation phase has the meaning given by subsection 187H(2).

service provider has the meaning given by subsection 187A(1).

6 At the end of subsection 6R(3)

Add "and all the enforcement agencies".

Part 3—Application provisions

7 Existing information and documents

(1) The amendments made by this Schedule apply in relation to information or a document:

(a) that is of a kind referred to in paragraph 187A(1)(a) or(b) of the *Telecommunications (Interception and Access) Act 1979* as amended by this Act; and

(b) that a service provider was keeping, or causing to be kept, immediately before the commencement of this item; and

(c) in relation to which a period specified in section 187C of that Act as so amended had not expired before that commencement.

(2) However, this item does not require a service provider to create, or to have created, any information or document that was not created by the operation, before that commencement, of a service to which Part 5-1A of that Act as so amended applies.

8 Reducing the period for keeping information or documents

(1) A service provider must not, before the commencement Part 5-1A of the *Telecommunications (Interception and Access) Act 1979* as amended by this Act, reduce the period for which it keeps or causes to be kept any information or document that the service provider will, after that commencement, be required by that Part to keep or cause to be kept.

(2) This item is taken to be a civil penalty provision for the purposes of the *Telecommunications Act 1997*, as if it had been so declared by a provision of that Act.

9 Applications made before commencement of Part 5-1A

(1) At any time after this Act receives the Royal Assent, a service provider may apply for either or both of the following:

(a) approval of:

(i) a data retention implementation plan; or

(ii) an amendment of a data retention implementation plan;

under Division 2 of Part 5-1A of the *Telecommunications (Interception and Access) Act 1979* as amended by this Act;

(b) a decision under subsection 187K(1) of that Act as so amended.

(2) Paragraph (1)(a) of this item does not apply to an application for approval of a data retention implementation plan unless the application would, if made after the commencement of Part 5-1A of that Act as so amended, have complied with section 187E of that Act as so amended.

10 Decisions made before commencement of Part 5-1A

(1) To avoid doubt, the power to make a decision under section 187F, 187G, 187J or 187K of the *Telecommunications (Interception and Access) Act 1979* as amended by this Act is taken, for the purposes of section 4 of the *Acts Interpretation Act 1901*, to be a power to make an instrument of an administrative character.

(2) Subsection 187F(3) of the *Telecommunications (Interception and Access) Act 1979* as amended by this Act applies, in relation to an application made before the commencement of Part 5-1A of that Act as so amended for approval of a data retention implementation plan, as if references in that subsection to 60 days were references to the number of days provided for in subitem (4) of this item.

(3) Paragraph 187K(5)(b) of the *Telecommunications (Interception and Access) Act 1979* as amended by this Act applies, in relation to an application made before the commencement of Part 5-1A of that Act as so amended for a decision under subsection 187K(1) of that Act as so amended, as if references in that paragraph to 60 days were references to the number of days provided for in subitem (4) of this item.

(4) For the purposes of subitem (2) or (3), the number of days is:

(a) the number of days in the period between:

(i) the day the application referred to in that subitem was made; and

(ii) the day immediately before the commencement of Part 5-1A of the *Telecommunications (Interception and Access) Act 1979* as amended by this Act; or

(b) 60 days;

whichever is the greater.

11 Keeping information or documents before commencement of Part 5-1A

A service provider may, before the commencement of this item, keep or cause to be kept any information or document that, after that commencement, Part 5-1A of the *Telecommunications (Interception and Access) Act 1979* as amended by this Act will require the service provider to keep or cause to be kept.

Schedule 2—Restricting access to stored communications and telecommunications data

Part 1—Main amendments

Telecommunications (Interception and Access) Act 1979

1 Subparagraphs 107J(1)(a)(i) and (ii)

Omit "an enforcement agency", substitute "a criminal law-enforcement agency".

2 Subsection 110(1)

Omit "An enforcement agency", substitute "A criminal law-enforcement agency".

3 After section 110

Insert:

110A Meaning of *criminal law-enforcement agency*

(1) Each of the following is a ***criminal law-enforcement agency***:

(a) the Australian Federal Police;

(b) a Police Force of a State;

(c) the Australian Commission for Law Enforcement Integrity;

(d) the ACC;

(e) the Australian Customs and Border Protection Service;

(f) the Crime Commission;

(g) the Independent Commission Against Corruption;

(h) the Police Integrity Commission;

(i) the IBAC;

(j) the Crime and Corruption Commission of Queensland;

(k) the Corruption and Crime Commission;

(l) the Independent Commissioner Against Corruption;

(m) subject to subsection (7), an authority or body for which a declaration under subsection (3) is in force.

(2) The head of an authority or body may request the Minister to declare the authority or body to be a criminal law-enforcement agency.

(3) The Minister may, by legislative instrument, declare:
  (a) the authority or body to be a criminal law-enforcement agency; and
  (b) persons specified, or of a kind specified, in the declaration to be officers of the criminal law-enforcement agency for the purposes of this Act.

(4) In considering whether to make the declaration, the Minister must have regard to:
  (a) whether the functions of the authority or body include investigating serious contraventions; and
  (b) whether access to stored communications, and the making of authorisations under section 180, would be reasonably likely to assist the authority or body in investigating those serious contraventions; and
  (c) whether the authority or body:
    (i) is required to comply with the Australian Privacy Principles; or
    (ii) is required to comply with a binding scheme that provides a level of protection of personal information that is comparable to the level provided by the Australian Privacy Principles; or
    (iii) has agreed in writing to comply with a scheme providing such a level of protection of personal information, in relation to personal information disclosed to it under Chapter 3 or 4, if the declaration is made; and
  (d) whether the authority or body proposes to adopt processes and practices that would ensure its compliance with the obligations of a criminal law-enforcement agency under Chapter 3, and the obligations of an enforcement agency under Chapter 4; and
  (e) whether the Minister considers that the declaration would be in the public interest; and
  (f) any other matter that the Minister considers relevant.

(5) In considering whether to make the declaration, the Minister may consult such persons or bodies as the Minister thinks fit. In particular, the Minister may consult the Privacy Commissioner and the Ombudsman.

(6) The declaration may be subject to conditions.

(7) Without limiting subsection (6), a condition may provide that the authority or body is not to exercise:

(a) a power conferred on a criminal law-enforcement agency by or under a specified provision in Chapter 3; or

(b) a power conferred on an enforcement agency by or under a specified provision in Chapter 4.

The authority or body is taken, for the purposes of this Act, not to be a criminal law-enforcement agency for the purposes of that provision in Chapter 3, or an enforcement agency for the purposes of that provision in Chapter 4, as the case requires.

(8) The Minister may, by legislative instrument, revoke a declaration under subsection (3) relating to an authority or body if the Minister is no longer satisfied that the circumstances justify the declaration remaining in force.

(9) The revocation under subsection (8) of a declaration relating to an authority or body does not affect the validity of:

(a) a domestic preservation notice given by the authority or body; or

(b) a stored communications warrant issued to the authority or body; or

(c) an authorisation made by an authorised officer of the authority or body under Division 4 of Part 4-1;

that was in force immediately before the revocation took effect.

4 Before section 177

Insert:

176A Meaning of *enforcement agency*

(1) Each of the following is an ***enforcement agency***:

(a) subject to subsection 110A(7), a criminal law-enforcement agency;
(b) subject to subsection (7), an authority or body for which a declaration under subsection (3) is in force.

(2) The head of an authority or body may request the Minister to declare the authority or body to be an enforcement agency.

(3) The Minister may, by legislative instrument, declare:
(a) the authority or body to be an enforcement agency; and
(b) persons specified, or of a kind specified, in the declaration to be officers of the enforcement agency for the purposes of this Act.

(4) In considering whether to make the declaration, the Minister must have regard to:
(a) whether the functions of the authority or body include:
(i) enforcement of the criminal law; or
(ii) administering a law imposing a pecuniary penalty; or
(iii) administering a law relating to the protection of the public revenue; and
(b) whether the making of authorisations under section 178 or 179 would be reasonably likely to assist the authority or body in performing those functions; and
(c) whether the authority or body:
(i) is required to comply with the Australian Privacy Principles; or
(ii) is required to comply with a binding scheme that provides a level of protection of personal information that is comparable to the level provided by the Australian Privacy Principles; or
(iii) has agreed in writing to comply with a scheme providing such a level of protection of personal information, in relation to personal information disclosed to it under Chapter 4, if the declaration is made; and
(d) whether the authority or body proposes to adopt processes and practices that would ensure its compliance with the obligations of an enforcement agency under Chapter 4; and

(e) whether the Minister considers that the declaration would be in the public interest; and

(f) any other matter that the Minister considers relevant.

(5) In considering whether to make the declaration, the Minister may consult such persons or bodies as the Minister thinks fit. In particular, the Minister may consult the Privacy Commissioner and the Ombudsman.

(6) The declaration may be subject to conditions.

(7) Without limiting subsection (6), a condition may provide that the authority or body is not to exercise a power conferred on an enforcement agency by or under a specified provision in Chapter 4. The authority or body is taken, for the purposes of this Act, not to be an enforcement agency for the purposes of that provision.

(8) The Minister may, by legislative instrument, revoke a declaration under subsection (3) relating to an authority or body if the Minister is no longer satisfied that the circumstances justify the declaration remaining in force.

(9) The revocation under subsection (8) of a declaration relating to an authority or body does not affect the validity of an authorisation, made by an authorised officer of the authority or body under this Division, that was in force immediately before the revocation took effect.

Part 2—Other amendments

Telecommunications (Interception and Access) Act 1979

5 Subsection 5(1) (definition of *Crime and Misconduct Commission*)

Omit "Misconduct", substitute "Corruption".

6 Subsection 5(1) (definition of *criminal law-enforcement agency*)

Repeal the definition, substitute:

criminal law-enforcement agency has the meaning given by section 110A.

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

Repeal the definition, substitute:

enforcement agency has the meaning given by section 176A.

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

Add:

; or (n) in the case of a criminal law-enforcement agency for which a declaration under subsection 110A(3) is in force—a person specified, or of a kind specified, in the declaration to be an officer of the criminal law-enforcement agency for the purposes of this Act; or

(o) in the case of an enforcement agency for which a declaration under subsection 176A(3) is in force—a person specified, or of a kind specified, in the declaration to be an officer of the enforcement agency for the purposes of this Act.

9 Section 107G

Omit "an enforcement agency or the Organisation", substitute "a criminal law-enforcement agency, or the Organisation,".

10 Section 107G

Omit "an interception agency or the Organisation", substitute "a criminal law-enforcement agency that is an interception agency, or the Organisation,".

11 Subsection 107J(1) (heading)

Repeal the heading, substitute:

Notices given by criminal law-enforcement agencies

12 Paragraphs 107L(2)(a), 107M(1)(a), (2)(a) and (3)(a)

Omit "an enforcement agency", substitute "a criminal law-enforcement agency".

13 Part 3-3 (heading)

Repeal the heading, substitute:

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

14 Section 110 (heading)

Repeal the heading, substitute:

110 Criminal law-enforcement agencies may apply for stored communications warrants

15 Subsections 111(3) and 116(1)

Omit "an enforcement agency", substitute "a criminal law-enforcement agency".

16 Subparagraph 120(1)(a)(i)

Omit "enforcement agency", substitute "criminal law-enforcement agency".

17 Subsection 120(2)

Omit "an enforcement agency's", substitute "a criminal law-enforcement agency's".

18 Subparagraph 120(2)(b)(ii)

Omit "enforcement agency", substitute "criminal law-enforcement agency".

19 Paragraph 120(3)(a)

Omit "enforcement agency's", substitute "criminal law-enforcement agency's".

20 Paragraph 120(3)(a)

Omit "enforcement agency", substitute "criminal law-enforcement agency".

21 Subsection 120(4)

Omit "enforcement agency", substitute "criminal law-enforcement agency".

22 Subsection 122(1)

Omit "an enforcement agency", substitute "a criminal law-enforcement agency".

23 Paragraph 122(1)(a)

Omit "enforcement agency", substitute "criminal law-enforcement agency".

24 Subsection 122(2)

Omit "an enforcement agency", substitute "a criminal law-enforcement agency".

25 Subsection 122(2)

Omit "other enforcement agency", substitute "other criminal law-enforcement agency".

26 Subsection 122(3)

Omit "an enforcement agency", substitute "a criminal law-enforcement agency".

27 Subsection 123(1)

Omit "an enforcement agency", substitute "a criminal law-enforcement agency".

28 Subsection 123(1)

Omit "other enforcement agency", substitute "other criminal law-enforcement agency".

29 Subsection 123(2)

Omit "enforcement agency", substitute "criminal law-enforcement agency".

30 Subsection 127(2)

Omit "an enforcement agency" (wherever occurring), substitute "a criminal law-enforcement agency".

31 Paragraphs 127(2)(a) and (b)

Omit "enforcement agency", substitute "criminal law-enforcement agency".

32 Subsections 127(3) and 128(1)

Omit "an enforcement agency", substitute "a criminal law-enforcement agency".

33 Subsection 128(3)

Omit "an enforcement agency" (wherever occurring), substitute "a criminal law-enforcement agency".

34 Section 130 (heading)

Repeal the heading, substitute:

130 Evidentiary certificates relating to actions by criminal law-enforcement agencies

35 Subsections 130(1) and (2)

Omit "an enforcement agency", substitute "a criminal law-enforcement agency".

36 Section 131

Omit "an enforcement agency", substitute "a criminal law-enforcement agency".

37 Subsection 135(1) (heading)

Repeal the heading, substitute:

Communicating information to the appropriate criminal law-enforcement agency

38 Paragraph 135(1)(a)

Omit "enforcement agency", substitute "criminal law-enforcement agency".

39 Subsection 135(2)

Omit "an enforcement agency", substitute "a criminal law-enforcement agency".

40 Section 138 (heading)

Repeal the heading, substitute:

138 Employee of carrier may communicate information to criminal law-enforcement agency

41 Subsection 138(2)

Omit "enforcement agency", substitute "criminal law-enforcement agency".

42 Subsection 139(1)

Omit "an enforcement agency", substitute "a criminal law-enforcement agency".

43 Paragraph 139(2)(a)

Omit "enforcement agency", substitute "criminal law-enforcement agency".

44 Paragraph 150(1)(a)

Omit "an enforcement agency's", substitute "a criminal law-enforcement agency's".

45 Subsections 159(1) and 160(1)

Omit "an enforcement agency", substitute "a criminal law-enforcement agency".

46 Subsections 161A(1) and (2) and 162(1)

Omit "enforcement agency", substitute "criminal law-enforcement agency".

47 Section 163

Omit "enforcement agency", substitute "criminal law-enforcement agency".

Part 3—Application provisions

48 Existing domestic preservation notices

If:

(a) a domestic preservation notice was given to a carrier before the commencement of this Schedule; and

(b) the notice was in force immediately before that commencement; and

(c) the authority or body that gave the notice was not the Organisation; and

(d) on that commencement, the authority or body is not a criminal law-enforcement agency (whether or not it is an enforcement agency);

after that commencement, the notice continues in force, and Chapter 3 of the *Telecommunications (Interception and Access) Act 1979* as amended by this Act continues to apply in relation to the notice, as if the authority or body were a criminal law-enforcement agency.

49 Existing stored communications warrants

If:

(a) a stored communications warrant was issued to an authority or body before the commencement of this Schedule; and

(b) the warrant was in force immediately before that commencement; and

(c) on that commencement, the authority or body is not a criminal law-enforcement agency (whether or not it is an enforcement agency);

after that commencement, the warrant continues in force, and Chapter 3 of the *Telecommunications (Interception and Access) Act 1979* as amended by this Act continues to apply in relation to the warrant, as if the authority or body were a criminal law-enforcement agency.

50 Existing authorisations

If:

(a) an authority or body made an authorisation under Division 4 of Part 4-1 of the *Telecommunications (Interception and*

Access) Act 1979 before the commencement of this Schedule; and

(b) the authorisation was in force immediately before that commencement; and

(c) on that commencement, the authority or body is not an enforcement agency;

after that commencement, the authorisation continues in force, and Chapter 4 of the *Telecommunications (Interception and Access) Act 1979* as amended by this Act continues to apply in relation to the authorisation, as if the authority or body were an enforcement agency.

51 Evidentiary certificates

(1) If:

(a) an authority or body issued a certificate under section 107U or 130 of the *Telecommunications (Interception and Access) Act 1979* before the commencement of this Schedule; and

(b) on that commencement, the authority or body is not a criminal law-enforcement agency (whether or not it is an enforcement agency);

after that commencement, the certificate continues in force as if the authority or body were a criminal law-enforcement agency.

(2) If:

(a) an authority or body issued a certificate under section 185C of the *Telecommunications (Interception and Access) Act 1979* before the commencement of this Schedule; and

(b) on that commencement, the authority or body is not an enforcement agency;

after that commencement, the certificate continues in force as if the authority or body were an enforcement agency.

(3) An authority or body that:

(a) was a criminal law-enforcement agency immediately before the commencement of this Schedule; and

(b) on that commencement, is not a criminal law-enforcement agency (whether or not it is an enforcement agency);

continues after that commencement to have the power to issue certificates under section 107U or 130 of the *Telecommunications (Interception and Access) Act 1979* as amended by this Act, with respect to anything done before that commencement, as if it were a criminal law-enforcement agency.

(4) An authority or body that:

(a) was an enforcement agency immediately before the commencement of this Schedule; and

(b) on that commencement, is not an enforcement agency;

continues after that commencement to have the power to issue certificates under section 185C of the *Telecommunications (Interception and Access) Act 1979* as amended by this Act, with respect to anything done before that commencement, as if it were an enforcement agency.

Schedule 3—Oversight by the Commonwealth Ombudsman

Part 1—Amendments

Telecommunications (Interception and Access) Act 1979

1 Subsection 5C(1)

Omit "or 3-5", substitute "or Chapter 4A".

2 At the end of section 87

Add:

(6) A person must not refuse:

(a) to attend before a person; or

(b) to give information; or

(c) to answer questions;

when required to do so under this section.

Penalty for an offence against this subsection: Imprisonment for 6 months.

3 Section 134

After "or 3-6", insert "or Chapter 4A".

4 Part 3-5 (heading)

Repeal the heading, substitute:

Part 3-5—Keeping and inspection of records

5 Divisions 1 and 2 of Part 3-5

Repeal the Divisions, substitute:

Division 1—Obligation to keep records

151 Obligation to keep records

(1) The chief officer of a criminal law-enforcement agency must cause the following, or copies of the following, to be kept in the agency's records for the period specified in subsection (3):

(a) each preservation notice given by the agency, and documents or other materials that indicate whether the notice was properly given;

(b) each notice under subsection 107L(3) of the revocation of such a preservation notice, and documents or other materials that indicate whether the revocation was properly made;

(c) each stored communications warrant issued to the agency, and documents or other materials that indicate whether the warrant was properly applied for, including:

(i) a copy of each application for such a warrant; and

(ii) a copy of each affidavit supporting such an application; and

(iii) documents or other materials that indicate whether the applicant for such a warrant complied with the requirements of Division 1 of Part 3-3;

(d) each instrument revoking such a warrant under section 122, and documents or other materials that indicate whether the revocation was properly made;

(e) documents or other materials that indicate the persons approved under subsection 127(2), and the persons appointed under subsection 127(3) to be approving officers for the purposes of subsection 127(2);

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

(g) each request for mutual assistance, being a request to which a mutual assistance application relates, and documents or other materials that indicate:

(i) whether the request was made lawfully; or

(ii) the offence in relation to which the request was made;

(h) documents or other materials that indicate whether the communication, use or recording of lawfully accessed

information (other than foreign intelligence information, preservation notice information or stored communication warrant information) complied with the requirements of Division 2 of Part 3-4;

(i) documents indicating whether information or a record was destroyed in accordance with section 150;

(j) each evidentiary certificate issued under this Chapter;

(k) each report given to the Minister under Division 1 of Part 3-6;

(l) documents and other materials of a kind prescribed under subsection (2) of this section.

(2) The Minister may, by legislative instrument, prescribe kinds of documents and other materials that the chief officer of a criminal law-enforcement agency must cause to be kept in the agency's records.

(3) The period for which the chief officer of a criminal law-enforcement agency must cause a particular item to be kept in the agency's records under subsection (1) of this section is the period:

(a) starting when the item came into existence; and

(b) ending:

(i) when 3 years have elapsed since the item came into existence; or

(ii) when the Ombudsman gives a report to the Minister under section 186J that is about records that include the item;

whichever happens earlier.

6 At the end of Part 4-2

Add:

186A Obligation to keep records

(1) The chief officer of an enforcement agency must cause the following, or copies of the following, to be kept in the agency's records for the period specified in subsection (3):

(a) each authorisation made by an authorised officer of the agency under section 178, 178A, 179 or 180, and documents or other materials that indicate any of the following:
  (i) whether the authorisation was properly made (including whether the authorised officer took into account the matters referred to in subsection 178(3), 178A(3), 179(3) or 180(4) (as the case requires), the matters referred to in section 180F and all other relevant considerations);
  (ii) if the authorisation is made under section 180—the period during which the authorisation is in force;
  (iii) when the authorisation was notified under subsection 184(3);
(b) each notice of the revocation under subsection 180(7) of an authorisation under section 180, and documents or other materials that indicate any of the following:
  (i) whether the revocation was properly made;
  (ii) when the revocation was notified under subsection 184(4);
(c) if the agency is the Australian Federal Police—each authorisation made by an authorised officer of the Australian Federal Police under section 180A or 180B, and documents or other materials that indicate any of the following:
  (i) whether the authorisation was properly made (including whether the authorised officer took into account the matters referred to in subsection 180A(3) or (5), 180B(3) or (8) or 180E(1) (as the case requires), the matters referred to in section 180F and all other relevant considerations);
  (ii) if the authorisation is made under section 180B—the period during which the authorisation is in force;
  (iii) if the authorisation is made under subsection 180B(8)—whether the authorised officer was satisfied as to the matters referred to in paragraphs 180B(8)(a) and (b);
  (iv) when the authorisation was notified under subsection 184(5);
(d) if the agency is the Australian Federal Police—each notice of the extension under subsection 180B(6) of an authorisation

under section 180B, and documents or other materials that indicate any of the following:

(i) whether the extension was properly made;

(ii) when the extension was notified under subsection 184(5);

(e) if the agency is the Australian Federal Police—each notice of the revocation under subsection 180B(4) of an authorisation under section 180B, and documents or other materials that indicate any of the following:

(i) whether the revocation was properly made;

(ii) when the revocation was notified under subsection 184(6);

(f) if the agency is the Australian Federal Police—each authorisation made by an authorised officer of the Australian Federal Police under section 180C or 180D, and documents or other materials that indicate whether the authorisation was properly made, including whether the authorised officer took into account:

(i) the matters referred to in subsection 180C(2), 180D(2) or 180E(1) (as the case requires); and

(ii) the matters referred to in section 180F; and

(iii) all other relevant considerations;

(g) documents or other materials that indicate whether:

(i) a disclosure of information or a document to which subsection 181B(1) or (2) applies took place in circumstances referred to in subsection 181B(3); or

(ii) a use of information or a document to which subsection 181B(4) or (5) applies took place in circumstances referred to in subsection 181B(6); or

(iii) a disclosure or use of information or a document to which subsection 182(1) applies took place in circumstances referred to in subsection 182(2), (2A), (3), (4) or (4A);

(h) each evidentiary certificate issued under section 185C;

(i) each report given to the Minister under section 186;

(j) documents and other materials of a kind prescribed under subsection (2) of this section.

(2) The Minister may, by legislative instrument, prescribe kinds of documents and other materials that the chief officer of an enforcement agency must cause to be kept in the agency's records.

(3) The period for which the chief officer of an enforcement agency must cause a particular item to be kept in the agency's records under subsection (1) of this section is the period:

(a) starting when the item came into existence; and

(b) ending:

(i) when 3 years have elapsed since the item came into existence; or

(ii) when the Ombudsman gives a report to the Minister under section 186J that is about records that include the item;

whichever happens earlier.

(4) Subsection (3) does not affect the operation of section 185.

7 Before Chapter 5

Insert:

Chapter 4A—Oversight by the Commonwealth Ombudsman

186B Inspection of records

(1) The Ombudsman must inspect records of an enforcement agency to determine:

(a) the extent of compliance with Chapter 4 by the agency and its officers; and

(b) if the agency is a criminal law-enforcement agency—the extent of compliance with Chapter 3 by the agency and its officers.

(2) For the purpose of an inspection under this section, the Ombudsman:

(a) after notifying the chief officer of the agency, may enter at any reasonable time premises occupied by the agency; and

(b) is entitled to have full and free access at all reasonable times to all records of the agency that are relevant to the inspection; and

(c) despite any other law, is entitled to make copies of, and to take extracts from, records of the agency; and

(d) may require a member of staff of the agency to give the Ombudsman any information that the Ombudsman considers necessary, being information:

(i) that is in the member's possession, or to which the member has access; and

(ii) that is relevant to the inspection.

(3) Before inspecting records of an enforcement agency under this section, the Ombudsman must give reasonable notice to the chief officer of the agency of when the inspection will occur.

(4) The chief officer must ensure that members of staff of the agency give the Ombudsman any assistance the Ombudsman reasonably requires to enable the Ombudsman to perform functions under this section.

(5) To avoid doubt, subsection (1) does not require the Ombudsman to inspect all of the records of an enforcement agency that are relevant to the matters referred to in paragraphs (1)(a) and (b).

(6) While an operation is being conducted under:

(a) a stored communications warrant; or

(b) an authorisation under Division 3, 4 or 4A of Part 4-1;

the Ombudsman may refrain from inspecting any records of the agency concerned that are relevant to the obtaining or execution of the warrant or authorisation.

186C Power to obtain relevant information

(1) If the Ombudsman has reasonable grounds to believe that an officer of a particular enforcement agency is able to give information relevant to an inspection under this Chapter of the agency's records, the Ombudsman may:

(a) if the Ombudsman knows the officer's identity—by writing given to the officer, require the officer to do one or both of the following:

(i) give the information to the Ombudsman, by writing signed by the officer, at a specified place and within a specified period;

(ii) attend before a specified inspecting officer to answer questions relevant to the inspection; or

(b) if the Ombudsman does not know the officer's identity—require the chief officer of the agency, or a person nominated by the chief officer, to attend before a specified inspecting officer to answer questions relevant to the inspection.

(2) A requirement under subsection (1) to attend before an inspecting officer must specify:

(a) a place for the attendance; and

(b) a period within which, or a time and day when, the attendance is to occur.

The place, and the period or the time and day, must be reasonable having regard to the circumstances in which the requirement is made.

(3) A person must not refuse:

(a) to attend before a person; or

(b) to give information; or

(c) to answer questions;

when required to do so under this section.

Penalty for an offence against this subsection: Imprisonment for 6 months.

186D Ombudsman to be given information and access despite other laws

(1) Despite any other law, a person is not excused from giving information, answering a question, or giving access to a document, as and when required under this Chapter, on the ground that giving the information, answering the question, or giving access to the document, as the case may be, would:

(a) contravene a law; or

(b) be contrary to the public interest; or

(c) might tend to incriminate the person or make the person liable to a penalty.

(2) However:

(a) the information, the answer, or the fact that the person has given access to the document, as the case may be; and

(b) any information or thing (including a document) obtained as a direct or indirect consequence of giving the information, answering the question or giving access to the document;

is not admissible in evidence against the person except in a proceeding by way of a prosecution for an offence against section 133, 181A, 181B or 182, or against Part 7.4 or 7.7 of the *Criminal Code*.

(3) Nothing in section 133, 181A, 181B or 182, or in any other law, prevents an officer of an enforcement agency from:

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

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

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

(4) Nothing in section 133, 181A, 181B or 182, or in any other law, prevents an officer of an enforcement agency from making a record of information, or causing a record of information to be made, for the purposes of giving the information to a person as permitted by subsection (3).

186E Application of Ombudsman Act

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

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

(3) Subject to section 186D of this Act, subsections 35(2), (3), (4) and (8) of the *Ombudsman Act 1976* apply for the purposes of this Chapter and so apply as if:

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

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

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

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

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

186F Exchange of information between Ombudsman and State inspecting authorities

(1) If the Ombudsman has obtained under this Act information relating to an authority of a State or Territory, the Ombudsman may give the information to another authority of that State or Territory (an ***inspecting authority***) that:

(a) has powers under the law of that State or Territory; and

(b) has the function of making inspections of a similar kind to those provided for in section 186B of this Act when the inspecting authority is exercising those powers.

(2) However, the Ombudsman may give the information only if the Ombudsman is satisfied that giving the information is necessary to enable the inspecting authority to perform its functions in relation to the authority of the State or Territory.

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

186G Delegation by Ombudsman

(1) The Ombudsman may delegate:

(a) to an APS employee responsible to the Ombudsman; or

(b) to a person having similar oversight functions to the Ombudsman under the law of a State or Territory or to an employee responsible to that person;

all or any of the Ombudsman's powers under this Chapter other than a power to report to the Minister.

(2) A delegate must, upon request by a person affected by the exercise of any power delegated to the delegate, produce the instrument of delegation, or a copy of the instrument, for inspection by the person.

186H Ombudsman not to be sued

The Ombudsman, an inspecting officer, or a person acting under an inspecting officer's direction or authority, is not liable to an action, suit or proceeding for or in relation to an act done, or omitted to be done, in good faith in the performance or exercise, or the purported performance or exercise, of a function or power conferred by this Chapter.

186J Reports

(1) The Ombudsman must report to the Minister, in writing, about the results of inspections under section 186B of the records of agencies during a financial year.

(2) The report under subsection (1) must be given to the Minister as soon as practicable after the end of the financial year.

(3) The Minister must cause a copy of the report to be laid before each House of the Parliament within 15 sitting days of that House after the Minister receives it.

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

(5) If, as a result of an inspection under this Chapter of the records of an enforcement agency, the Ombudsman is of the opinion that an officer of the agency has contravened a provision of this Act, the Ombudsman may include in his or her report on the inspection a report on the contravention.

Note: In complying with this section, the Ombudsman remains bound by the obligations imposed by sections 133, 181B and 182.

(6) The Ombudsman must give a copy of a report under subsection (1) or (4) to the chief officer of any enforcement agency to which the report relates.

(7) A report under this section must not include information which, if made public, could reasonably be expected to:

(a) endanger a person's safety; or

(b) prejudice an investigation or prosecution; or

(c) compromise any enforcement agency's operational activities or methodologies.

Part 2—Application provisions

8 Existing inspections by the Ombudsman

If an inspection that the Ombudsman was conducting before the commencement of this Schedule under section 152 of the *Telecommunications (Interception and Access) Act 1979* was not finished before that commencement, after that commencement:

(a) the inspection is taken to be an inspection conducted under Chapter 4A of that Act as amended by this Act; and

(b) anything done under that section in relation to the inspection before that commencement is taken to have been done under Chapter 4A of that Act as so amended.

9 Reports

If:

(a) an inspection that the Ombudsman was conducting before the commencement of this Schedule under section 152 of the *Telecommunications (Interception and Access) Act 1979* was finished before that commencement; but

(b) the inspection was not the dealt with before that commencement in any report to the Minister under section 153 of that Act;

section 186J of that Act as amended by this Act applies in relation to the inspection as if it had been conducted under section 186B of that Act as so amended.

10 Obligation to keep records

(1) Sections 151 and 186A of the *Telecommunications (Interception and Access) Act 1979* as amended by this Act do not apply in relation to anything done before the commencement of this Schedule.

(2) Despite the repeal of sections 150A and 151 of the *Telecommunications (Interception and Access) Act 1979* by this Act, those sections continue to apply in relation to things done before the commencement of this Schedule as if those sections had not been repealed.