The Parliament of the Commonwealth of Australia

HOUSE OF REPRESENTATIVES

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

(Government)

(1) Schedule 1, item 1, page 3 (line 11), after “to be kept,”, insert “in accordance with section 187BA and”.

[encryption and protection of information]

(2) Schedule 1, item 1, page 3 (line 13), omit “prescribed by the regulations”, substitute “specified in or under section 187AA”.

[information to be kept]

(3) Schedule 1, item 1, page 3 (line 22) to page 4 (line 9), omit subsection 187A(2).

[information to be kept]

(4) Schedule 1, item 1, page 4 (line 19), omit “prescribed by the regulations”, substitute “for which a declaration under subsection (3A) is in force”.

[declared services]

(5) Schedule 1, item 1, page 4 (after line 24), after subsection 187A(3), insert:

(3A) The Minister may, by legislative instrument, declare a service to be a service to which this Part applies.

(3B) A declaration under subsection (3A):

(a) comes into force when it is made, or on such later day as is specified in the declaration; and

(b) ceases to be in force at the end of the period of 40 sitting days of a House of the Parliament after the declaration comes into force.

(3C) If a Bill is introduced into either House of the Parliament that includes an amendment of subsection (3), the Minister:

(a) must refer the amendment to the Parliamentary Joint Committee on Intelligence and Security for review; and

(b) must not in that referral specify, as the period within which the Committee is to report on its review, a period that will end earlier than 15 sitting days of a House of the Parliament after the introduction of the Bill.

[declared services; declarations ceasing to be in force]
(6) Schedule 1, item 1, page 5 (lines 6 to 11), omit paragraph 187A(4)(c), substitute:
  (c) information to the extent that it relates to a communication that is being carried by
  means of another service:
  (i) that is of a kind referred to in paragraph (3)(a); and
  (ii) that is operated by another person using the relevant service operated by the
  service provider;
  or a document to the extent that the document contains such information; or
  
  Note: This paragraph puts beyond doubt that service providers are not required to keep information 
or documents about communications that pass “over the top” of the underlying service they 
provide, and that are being carried by means of other services operated by other service 
providers.

[“over the top” services]

(7) Schedule 1, item 1, page 6 (lines 3 to 6), omit subsection 187A(7).

[Information to be kept]

(8) Schedule 1, item 1, page 6 (after line 6), after section 187A, insert:

187AA Information to be kept

(1) The following table sets out the kinds of information that a service provider must keep, or 
cause to be kept, under subsection 187A(1):

<table>
<thead>
<tr>
<th>Item</th>
<th>Topic Column 1</th>
<th>Description of information Column 2</th>
</tr>
</thead>
</table>
| 1    | The subscriber of, and accounts, services, telecommunications devices and other relevant services relating to, the relevant service | The following:
|      |                | (a) any information that is one or both of the following:
|      |                |   (i) any name or address information; 
|      |                |   (ii) any other information for identification purposes; 
|      |                | relating to the relevant service, being information used by the service provider for the purposes of identifying the subscriber of the relevant service; 
|      |                | (b) any information relating to any contract, agreement or arrangement relating to the relevant service, or to any related account, service or device; 
|      |                | (c) any information that is one or both of the following:
|      |                |   (i) billing or payment information; 
|      |                |   (ii) contact information; 
|      |                | relating to the relevant service, being information used by the service provider in relation to the relevant service; 
|      |                | (d) any identifiers relating to the relevant service or any related account, service or device, being information used by the service provider in relation to the relevant service or any related account, service or device; |
## Kinds of information to be kept

<table>
<thead>
<tr>
<th>Item</th>
<th>Topic Column 1</th>
<th>Description of information Column 2</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>(e) the status of the relevant service, or any related account, service or device.</td>
</tr>
<tr>
<td>2</td>
<td>The source of a communication</td>
<td>Identifiers of a related account, service or device from which the communication has been sent by means of the relevant service.</td>
</tr>
<tr>
<td>3</td>
<td>The destination of a communication</td>
<td>Identifiers of the account, telecommunications device or relevant service to which the communication: (a) has been sent; or (b) has been forwarded, routed or transferred, or attempted to be forwarded, routed or transferred.</td>
</tr>
<tr>
<td>4</td>
<td>The date, time and duration of a communication, or of its connection to a relevant service</td>
<td>The date and time (including the time zone) of the following relating to the communication (with sufficient accuracy to identify the communication): (a) the start of the communication; (b) the end of the communication; (c) the connection to the relevant service; (d) the disconnection from the relevant service.</td>
</tr>
<tr>
<td>5</td>
<td>The type of a communication or of a relevant service used in connection with a communication</td>
<td>The following: (a) the type of communication; Examples: Voice, SMS, email, chat, forum, social media. (b) the type of the relevant service; Examples: ADSL, Wi-Fi, VoIP, cable, GPRS, VoLTE, LTE. (c) the features of the relevant service that were, or would have been, used by or enabled for the communication. Examples: Call waiting, call forwarding, data volume usage. Note: This item will only apply to the service provider operating the relevant service: see paragraph 187A(4)(c).</td>
</tr>
<tr>
<td>6</td>
<td>The location of equipment, or a line, used in connection with a communication</td>
<td>The following in relation to the equipment or line used to send or receive the communication: (a) the location of the equipment or line at the start of the communication; (b) the location of the equipment or line at the end of the communication. Examples: Cell towers, Wi-Fi hotspots.</td>
</tr>
</tbody>
</table>

(2) The Minister may, by legislative instrument, make a declaration modifying (including by adding, omitting or substituting) the table in subsection (1), or that table as previously modified under this subsection.

(3) A declaration under subsection (2):
(a) comes into force when it is made, or on such later day as is specified in the declaration; and
(b) ceases to be in force at the end of the period of 40 sitting days of a House of the Parliament after the declaration comes into force.

(4) If a Bill is introduced into either House of the Parliament that includes an amendment of subsection 187A(4) or subsection (1) or (5) of this section, the Minister:
(a) must refer the amendment to the Parliamentary Joint Committee on Intelligence and Security for review; and
(b) must not in that referral specify, as the period within which the Committee is to report on its review, a period that will end earlier than 15 sitting days of a House of the Parliament after the introduction of the Bill.

(5) For the purposes of items 2, 3, 4 and 6 of the table in subsection (1) and any modifications of those items under subsection (2), 2 or more communications that together constitute a single communications session are taken to be a single communication.

[information to be kept]

(9) Schedule 1, item 1, page 6 (after line 21), after subsection 187B(2), insert:

(2A) Before making the declaration, the Communications Access Co-ordinator may consult the Privacy Commissioner.

[certain service providers not covered]

(10) Schedule 1, item 1, page 6 (after line 25), after paragraph 187B(3)(b), insert:

(ba) the objects of the Privacy Act 1988; and

(bb) any submissions made by the Privacy Commissioner because of the consultation under subsection (2A); and

[certain service providers not covered]

(11) Schedule 1, item 1, page 6 (after line 30), at the end of section 187B, add:

(6) As soon as practicable after making a declaration under subsection (2), the Communications Access Co-ordinator must give written notice of the declaration to the Minister.

(7) As soon as practicable after receiving the notice under subsection (6), the Minister must give written notice of the declaration to the Parliamentary Joint Committee on Intelligence and Security.

[notifying declarations of services]

(12) Schedule 1, item 1, page 6 (after line 30), after section 187B, insert:

187BA Ensuring the confidentiality of information

A service provider must protect the confidentiality of information that, or information in a document that, the service provider must keep, or cause to be kept, under section 187A by:

(a) encrypting the information; and

(b) protecting the information from unauthorised interference or unauthorised access.

[encryption and protection of information]
(13) Schedule 1, item 1, page 7 (line 6), omit “paragraph 187A(2)(a)”, substitute “paragraph (a) or (b) in column 2 of item 1 of the table in subsection 187AA(1)”.

[information to be kept]

(14) Schedule 1, item 1, page 7 (line 16), omit “paragraph 187A(2)(a)”, substitute “paragraph (a) or (b) in column 2 of item 1 of the table in subsection 187AA(1)”.

[information to be kept]

(15) Schedule 1, item 1, page 7 (line 31), omit “section 187C”, substitute “section 187BA or 187C”.

[encryption and protection of information]

(16) Schedule 1, item 1, page 8 (line 6), after “keeping”, insert “, and ensuring the confidentiality of.”.

[encryption and protection of information]

(17) Schedule 1, item 1, page 8 (line 11), after “keeping”, insert “, and ensuring the confidentiality of.”.

[encryption and protection of information]

(18) Schedule 1, item 1, page 8 (line 13), omit “section 187C”, substitute “sections 187BA and 187C”.

[encryption and protection of information]

(19) Schedule 1, item 1, page 8 (line 15), omit “section 187C”, substitute “sections 187BA and 187C”.

[encryption and protection of information]

(20) Schedule 1, item 1, page 9 (line 4), omit “section 187C”, substitute “sections 187BA and 187C”.

[encryption and protection of information]

(21) Schedule 1, item 1, page 9 (line 9), omit “section 187C”, substitute “section 187BA or 187C”.

[encryption and protection of information]

(22) Schedule 1, item 1, page 12 (line 1), omit “the end of”.

[technical correction]

(23) Schedule 1, item 1, page 13 (line 16), omit “exemption”, substitute “decision”.

[technical correction]

(24) Schedule 1, item 1, page 14 (line 19), after “data retention”, insert “or information security”.

[encryption and protection of information]

(25) Schedule 1, item 1, page 14 (after line 22), at the end of Division 3, add:

**187KA Review of exemption or variation decisions**

(1) A service provider may apply in writing to the ACMA for review of a decision under subsection 187K(1) relating to the service provider.

(2) The ACMA must:
(a) confirm the decision; or
(b) substitute for that decision another decision that could have been made under subsection 187K(1).

A substituted decision under paragraph (b) has effect (other than for the purposes of this section) as if it were a decision of the Communications Access Co-ordinator under subsection 187K(1).

(3) Before considering its review of the decision under subsection 187K(1), the ACMA must give a copy of the application to:
   (a) the Communications Access Co-ordinator; and
   (b) any enforcement agencies and security authorities that were given, under subparagraph 187K(5)(a)(i), a copy of the application for the decision under review; and
   (c) any other enforcement agencies and security authorities that, in the opinion of the ACMA, are likely to be interested in the application.

Matters to be taken into account

(4) Before making a decision under subsection (2) in relation to a service provider, the ACMA 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 or information security arrangements that the service provider has identified.

(5) The ACMA may take into account any other matter it considers relevant.

[review by the ACMA]

(26) Schedule 1, item 1, page 14 (before line 24), before section 187L, insert:

187KB Commonwealth may make a grant of financial assistance to service providers

(1) The Commonwealth may make a grant of financial assistance to a service provider for the purpose of assisting the service provider to comply with the service provider’s obligations under this Part.

(2) The terms and conditions on which that financial assistance is granted are to be set out in a written agreement between the Commonwealth and the service provider.

(3) An agreement under subsection (2) may be entered into on behalf of the Commonwealth by the Minister.

[financial assistance to service providers]

(27) Schedule 1, item 1, page 14 (after line 33), after subsection 187L(1), insert:

(1A) If the ACMA receives a service provider’s application under section 187KA for review of a decision under subsection 187K(1), the ACMA must:
   (a) treat the application as confidential; and
   (b) ensure that it is not disclosed to any other person or body (other than the Communications Access Co-ordinator, an enforcement agency or a security authority) without the written permission of the service provider.
(28) Schedule 1, item 1, page 15 (lines 1 and 2), omit “, an enforcement agency or a security
authority must, if it receives under paragraph 187G(1)(a) or 187K(5)(a)”, substitute “, the
Communications Access Co-ordinator, an enforcement agency or a security authority must, if
it receives under subsection 187G(1), paragraph 187K(5)(a) or subsection 187KA(3)”.

(29) Schedule 1, item 1, page 15 (after line 6), after section 187L, insert:

187LA Application of the Privacy Act 1988

(1) The Privacy Act 1988 applies in relation to a service provider, as if the service provider
were an organisation within the meaning of that Act, to the extent that the activities of the
service provider relate to retained data.

(2) Information that is kept under this Part, or information that is in a document kept under
this Part is taken, for the purposes of the Privacy Act 1988, to be personal information
about an individual if the information relates to:

(a) the individual; or

(b) a communication to which the individual is a party.

(30) Schedule 1, item 1, page 15 (lines 14 to 17), omit subsection 187N(1), substitute:

(1) The Parliamentary Joint Committee on Intelligence and Security must review the
operation of this Part.

(1A) The review:

(a) must start on or before the second anniversary of the end of the implementation
phase; and

(b) must be concluded on or before the third anniversary of the end of the
implementation phase.

(31) Schedule 1, item 1, page 15 (after line 19), at the end of section 187N, add:

(3) Until the review is completed, the head (however described) of an enforcement agency
must keep:

(a) all of the documents that he or she is required to retain under section 185; and

(b) all of the information that he or she is required, by paragraphs 186(1)(e) to (k), to
include in a report under subsection 186(1);
relating to the period starting on the commencement of this Part and ending when the
review is completed.

(4) Until the review is completed, the Director-General of Security must keep:

(a) all of the authorisations made under Division 3 of Part 4-1; and

(b) all of the information that he or she is required, by paragraphs 94(2A)(c) to (j) of
the Australian Security Intelligence Organisation Act 1979, to include in a report
referred to in subsection 94(1) of that Act;
relating to the period starting on the commencement of this Part and ending when the
review is completed.
(5) Subsections (3) and (4) do not limit any other obligation to keep information under this Act or another law.

[keeping information to assist review]

(32) Schedule 1, item 1, page 15 (after line 23), after subsection 187P(1), insert:

(1A) Without limiting the matters that may be included in a report under subsection (1), it must include information about:
   (a) the costs to service providers of complying with this Part; and
   (b) the use of data retention implementation plans approved under Division 2 of this Part.

[annual reports]

(33) Schedule 1, page 16 (after line 1), after the heading to Part 2, insert:

Australian Security Intelligence Organisation Act 1979

1A Section 4

Insert:

retained data has the same meaning as in the Telecommunications (Interception and Access) Act 1979.

[reports on access to data]

(34) Schedule 1, page 16, after proposed item 1A, insert:

1B Paragraphs 94(2A)(a) and (b)

Omit “year”, substitute “period”.

1C At the end of subsection 94(2A)

Add:
    ; and (c) the number of authorisations made during the period under section 175 and subsection 176(3) of the Telecommunications (Interception and Access) Act 1979; and
    (d) the purposes for which those authorisations were made; and
    (e) the lengths of time for which the information or documents that were, or would have been, covered by those authorisations had been held when access was sought; and
    (f) the number of those authorisations that related to retained data that included information of a kind referred to in item 1 of the table in subsection 187AA(1) of that Act; and
    (g) the number of those authorisations that related to retained data that included information of a kind referred to in item 2, 3, 4, 5 or 6 of the table in subsection 187AA(1) of that Act; and
    (h) the number of those authorisations that were made under journalist information warrants issued under Subdivision B of Division 4C of Part 4-1 of that Act; and
    (i) the number of journalist information warrants issued under that Subdivision during the period; and
    (j) information of a kind declared under subsection (2C) of this section.
1D After subsection 94(2A)

Insert:

(2B) A report under subsection (1) is to set out the matters referred to in paragraph (2A)(e) by specifying:

(a) in relation to each of 8 successive periods of 3 months, the number of the authorisations sought for information or documents held for lengths of time included in that period; and

(b) the number of the authorisations sought for information or documents held for lengths of time exceeding 24 months.

(2C) The Minister may, by legislative instrument, declare kinds of information that are to be set out in a report under subsection (1).

[reports on access to data]

(35) Schedule 1, page 16, after proposed item 1D, insert:

Intelligence Services Act 2001

1E Section 3

Insert:

*retained data activity* means an activity relating to information, or documents, that a service provider has been required to keep under Part 5-1A of the *Telecommunications (Interception and Access) Act 1979*.

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

[functions of the Parliamentary Joint Committee on Intelligence and Security]

(36) Schedule 1, page 16, after proposed item 1E, insert:

1F After paragraph 29(1)(bb)

Insert:

(bc) to conduct the review under section 187N of the *Telecommunications (Interception and Access) Act 1979*; and

(bd) subject to subsection (5), to review any matter that:

(i) relates to the retained data activities of ASIO; and

(ii) is included, under paragraph 94(2A)(c), (d), (e), (f), (g), (h), (i) or (j) of the *Australian Security Intelligence Organisation Act 1979*, in a report referred to in subsection 94(1) of that Act; and

(be) subject to subsection (5), to review any matter that:

(i) relates to the retained data activities of the AFP in relation to offences against Part 5.3 of the *Criminal Code*; and

(ii) is set out, under paragraph 186(1)(e), (f), (g), (h), (i), (j) or (k) of the *Telecommunications (Interception and Access) Act 1979*, in a report under subsection 186(1) of that Act; and

1G At the end of section 29

Add:
(4) Subject to subsection (5), paragraphs (3)(c) and (k) do not apply to things done in the performance of the Committee’s functions under paragraphs (1)(bd) and (be).

(5) The Committee’s functions under paragraphs (1)(bd) and (be):
   (a) are to be performed for the sole purpose of assessing, and making recommendations on, the overall operation and effectiveness of Part 5-1A of the Telecommunications (Interception and Access) Act 1979; and
   (b) do not permit reviewing the retained data activities of service providers; and
   (c) may not be performed for any purpose other than that set out in paragraph (a).

Note: The performance of the Committee’s functions under paragraphs (1)(bd) and (be) are also subject to the requirements of Schedule 1.

[functions of the Parliamentary Joint Committee on Intelligence and Security]

(37) Schedule 1, page 16, after proposed item 1G, insert:

Privacy Act 1988

1H Subsection 6(1) (at the end of the definition of personal information)

Add:

   Note: Section 187LA of the Telecommunications (Interception and Access) Act 1979 extends the meaning of personal information to cover information kept under Part 5-1A of that Act.

[personal information]

(38) Schedule 1, page 16, after proposed item 1H, insert:

1J Subsection 6C(1) (note)

Repeal the note, substitute:

   Note 1: Under section 187LA of the Telecommunications (Interception and Access) Act 1979, service providers are, in relation to their activities relating to retained data, treated as organisations for the purposes of this Act.

   Note 2: Regulations may prescribe an instrumentality by reference to one or more classes of instrumentality. See subsection 13(3) of the Legislative Instruments Act 2003.

[application of the Privacy Act]

(39) Schedule 1, page 16 (after line 17), after item 3, insert:

3A After subsection 280(1A)

Insert:

   (1B) Subject to subsection (1C), paragraph (1)(b) does not apply to a disclosure of information or a document if:
      (a) the disclosure is required or authorised because of:
         (i) a subpoena; or
         (ii) a notice of disclosure; or
         (iii) an order of a court;
      in connection with a civil proceeding; and
   (b) the information or document is kept, by a service provider (within the meaning of the Telecommunications (Interception and Access) Act 1979), solely for the purpose of complying with Part 5-1A of that Act; and
(c) the information or document is not used or disclosed by the service provider for any purpose other than one or more of the following purposes:
   (i) complying with Part 5-1A of that Act;
   (ii) complying with the requirements of warrants under Chapters 2 and 3 of that Act or authorisations under Chapter 4 of that Act;
   (iii) complying with requests or requirements to make disclosures provided for by sections 284 to 288 of this Act;
   (iv) providing persons with access to their personal information in accordance with the Privacy Act 1988;
   (v) a purpose prescribed by the regulations;
   (vi) a purpose incidental to any of the purposes referred to in subparagraphs (i) to (v).

(1C) Subsection (1B) does not apply:
   (a) in circumstances of a kind prescribed by the regulations; or
   (b) to a disclosure to an enforcement agency (within the meaning of the Telecommunications (Interception and Access) Act 1979); or
   (c) to a disclosure that occurs during the implementation phase (within the meaning of that Act).

[access to retained data]

(40) Schedule 1, page 16, after proposed item 3A, insert:

3B Section 281

Before “Division 2”, insert “(1)”.

3C At the end of section 281

Add:

(2) Subject to subsection (3), this section does not apply to a disclosure of information or a document by a person as a witness in a civil proceeding if the information or document:
   (a) is kept, by a service provider (within the meaning of the Telecommunications (Interception and Access) Act 1979), solely for the purpose of complying with Part 5-1A of that Act; and
   (b) is not used or disclosed by the service provider for any purpose other than one or more of the following purposes:
      (i) complying with Part 5-1A of that Act;
      (ii) complying with the requirements of warrants under Chapters 2 and 3 of that Act or authorisations under Chapter 4 of that Act;
      (iii) complying with requests or requirements to make disclosures provided for by sections 284 to 288 of this Act;
      (iv) providing persons with access to their personal information in accordance with the Privacy Act 1988;
      (v) a purpose prescribed by the regulations;
      (vi) a purpose incidental to any of the purposes referred to in subparagraphs (i) to (v).

(3) Subsection (2) does not apply:
   (a) in circumstances of a kind prescribed by the regulations; or
(b) to a disclosure to an enforcement agency (within the meaning of the Telecommunications (Interception and Access) Act 1979); or
(c) to a disclosure that occurs during the implementation phase (within the meaning of that Act).

[access to retained data]

(41) Schedule 1, item 5, page 16 (lines 24 to 28), omit the item, substitute:

5 Subsection 5(1)

Insert:

Defence Minister has the same meaning as in the Intelligence Services Act 2001.
Foreign Affairs Minister has the same meaning as in the Intelligence Services Act 2001.
IGIS official has the same meaning as in the Australian Security Intelligence Organisation Act 1979.
implementation phase has the meaning given by subsection 187H(2).
infrastructure means any line or equipment used to facilitate communications across a telecommunications network.
journalist information warrant means a warrant issued under Division 4C of Part 4-1.
Part 4-1 issuing authority means a person in respect of whom an appointment is in force under section 6DC.
Public Interest Advocate means a person declared under section 180X to be a Public Interest Advocate.
related account, service or device, in relation to a service to which Part 5-1A applies, means:
   (a) an account; or
   (b) a telecommunications device; or
   (c) another service of a kind referred to in paragraph 187A(3)(a); that is related to the service.
retained data means information, or documents, that a service provider is or has been required to keep under Part 5-1A.

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

source (except in item 2 of the table in subsection 187AA(1)) means a person who provides information:
   (a) to another person who is working in a professional capacity as a journalist; and
   (b) in the normal course of the other person’s work in such a capacity; and
   (c) in the expectation that the information may be disseminated in the form of:
       (i) news, current affairs or a documentary; or
       (ii) commentary or opinion on, or analysis of, news, current affairs or a documentary.

[warrants; IGIS; infrastructure; information to be kept; application of the Privacy Act; media sources]

(42) Schedule 1, page 17 (after line 2), at the end of Part 2, add:
6A After section 6DB

Insert:

6DC Part 4-1 issuing authorities

(1) The Minister may, by writing, appoint as a Part 4-1 issuing authority:
   (a) a person who is:
       (i) a judge of a court created by the Parliament; or
       (ii) a magistrate;
       and in relation to whom a consent under subsection (2) is in force; or
   (b) a person who:
       (i) holds an appointment to the Administrative Appeals Tribunal as Deputy
           President, full-time senior member, part-time senior member or member; and
       (ii) is enrolled as a legal practitioner of a federal court or of the Supreme Court of
           a State or a Territory; and
       (iii) has been enrolled for at least 5 years.

(2) A person who is:
   (a) a judge of a court created by the Parliament; or
   (b) a magistrate;
   may, by writing, consent to be appointed by the Minister under subsection (1).

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

(4) A Part 4-1 issuing authority has, in relation to the performance or exercise of a function
    or power conferred on a Part 4-1 issuing authority by this Act, the same protection and
    immunity as a Justice of the High Court has in relation to proceedings in the High Court.

(43) Schedule 1, page 17 (after proposed item 6A), at the end of Part 2, add:

6B Section 64 (heading)
Repeal the heading, substitute:

64 Dealing in connection with Organisation’s or Inspector-General’s functions

6C Subsection 64(1)
After “its functions”, insert “or the performance by the Inspector-General of Intelligence and
Security of his or her functions”.

6D Subsection 64(2)
Repeal the subsection, substitute:

(2) A person, being the Director-General of Security or an ASIO employee, ASIO affiliate or
    IGIS official, may:
    (a) in connection with the performance by the Organisation of its functions; or
(b) in connection with the performance by the Inspector-General of Intelligence and Security of his or her functions; communicate to another such person, make use of, or make a record of, foreign intelligence information.

[warrants]

(44) Schedule 1, page 17 (after proposed item 6D), at the end of Part 2, add:

**6E Paragraph 176(5)(b)**

Repeal the paragraph, substitute:

(b) unless it is revoked earlier, ends at the time specified in the authorisation, which must be a time that:

(i) is no later than the end of the period of 90 days beginning on the day the authorisation is made; and

(ii) if the authorisation is made under a journalist information warrant—is no later than the end of the period specified under section 180N as the period for which the warrant is to remain in force.

**6F Subsection 176(6)**

Repeal the subsection, substitute:

_Revoking the authorisation_

(6) An eligible person must revoke the authorisation if:

(a) he or she is satisfied that the disclosure is no longer required; or

(b) in a case where the authorisation is made under a journalist information warrant:

(i) the warrant is revoked under subsection 180N(1); or

(ii) the Director-General of Security has informed the Minister under section 180P that the Director-General is satisfied that the grounds on which the warrant was issued have ceased to exist.

Note: Section 184 deals with notification of authorisations.

[warrants]

(45) Schedule 1, page 17 (after proposed item 6F), at the end of Part 2, add:

**6G Paragraph 180(6)(b)**

Repeal the paragraph, substitute:

(b) unless it is revoked earlier, ends at the time specified in the authorisation, which must be a time that:

(i) is no later than the end of the period of 45 days beginning on the day the authorisation is made; and

(ii) if the authorisation is made under a journalist information warrant—is no later than the end of the period specified under subsection 180U(3) as the period for which the warrant is to remain in force.

**6H Subsection 180(7)**

Repeal the subsection, substitute:
Revoking the authorisation

(7) An authorised officer of the criminal law-enforcement agency must revoke the authorisation if:
   (a) he or she is satisfied that the disclosure is no longer required; or
   (b) in a case where the authorisation is made under a journalist information warrant—
       the warrant is revoked under subsection 180W(1).

Note: Section 184 deals with notification of authorisations.

[6J Section 180F]

Omit “have regard to whether any interference with the privacy of any person or persons that may result from the disclosure or use is justifiable”, substitute “be satisfied on reasonable grounds that any interference with the privacy of any person or persons that may result from the disclosure or use is justifiable and proportionate”.

[6K Before paragraph 180F(a)]

Insert:

(aa) the gravity of any conduct in relation to which the authorisation is sought, including:
   (i) the seriousness of any offence in relation to which the authorisation is sought; and
   (ii) the seriousness of any pecuniary penalty in relation to which the authorisation is sought; and
   (iii) the seriousness of any protection of the public revenue in relation to which the authorisation is sought; and
   (iv) whether the authorisation is sought for the purposes of finding a missing person;

[authorised officers to consider privacy]

[6L After Division 4B of Part 4-1]

Insert:

Division 4C—Journalist information warrants

Subdivision A—The requirement for journalist information warrants

180G The Organisation

(1) An eligible person (within the meaning of subsection 175(2) or 176(2), as the case requires) must not make an authorisation under Division 3 that would authorise the disclosure of information or documents relating to a particular person if:
   (a) the eligible person knows or reasonably believes that particular person to be:
       (i) a person who is working in a professional capacity as a journalist; or
       (ii) an employer of such a person; and
(b) a purpose of making the authorisation would be to identify another person whom the eligible person knows or reasonably believes to be a source; unless a journalist information warrant is in force in relation to that particular person.

(2) Nothing in this section affects by implication the kind of person in relation to whom a warrant (other than a journalist information warrant) may be issued under this Act.

180H Enforcement agencies

(1) An authorised officer of an enforcement agency must not make an authorisation under section 178, 178A, 179 or 180 that would authorise the disclosure of information or documents relating to a particular person if:
   (a) the authorised officer knows or reasonably believes that particular person to be:
       (i) a person who is working in a professional capacity as a journalist; or
       (ii) an employer of such a person; and
   (b) a purpose of making the authorisation would be to identify another person whom the authorised officer knows or reasonably believes to be a source; unless a journalist information warrant is in force, in relation to that particular person, under which authorised officers of the agency may make authorisations under that section.

(2) An authorised officer of the Australian Federal Police must not make an authorisation under Division 4A that would authorise the disclosure of information or documents relating to a particular person if:
   (a) the authorised officer knows or reasonably believes that particular person to be:
       (i) a person who is working in a professional capacity as a journalist; or
       (ii) an employer of such a person; and
   (b) a purpose of making the authorisation would be to identify another person whom the authorised officer knows or reasonably believes to be a source.

(3) Nothing in this section affects by implication the kind of person in relation to whom a warrant (other than a journalist information warrant) may be issued under this Act.

Subdivision B—Issuing journalist information warrants to the Organisation

180J Requesting a journalist information warrant

(1) The Director-General of Security may request the Minister to issue a journalist information warrant in relation to a particular person.

(2) The request must specify the facts and other grounds on which the Director-General considers it necessary that the warrant be issued.

180K Further information

(1) The Minister may require the Director-General of Security to give to the Minister, within the period specified in the requirement, further information in connection with a request under this Subdivision.

(2) If the Director-General breaches the requirement, the Minister may:
   (a) refuse to consider the request; or
   (b) refuse to take any action, or any further action, in relation to the request.
180L Issuing a journalist information warrant

(1) After considering a request under section 180J, the Minister must:
   (a) issue a journalist information warrant that authorises the making of authorisations under Division 3 in relation to the particular person to which the request relates; or
   (b) refuse to issue a journalist information warrant.

(2) The Minister must not issue a journalist information warrant unless the Minister is satisfied that:
   (a) the Organisation’s functions would extend to the making of authorisations under Division 3 in relation to the particular person; and
   (b) the public interest in issuing the warrant outweighs the public interest in protecting the confidentiality of the identity of the source in connection with whom authorisations would be made under the authority of the warrant, having regard to:
       (i) the extent to which the privacy of any person or persons would be likely to be interfered with by the disclosure of information or documents under authorisations that are likely to be made under the authority of the warrant; and
       (ii) the gravity of the matter in relation to which the warrant is sought; and
       (iii) the extent to which that information or those documents would be likely to assist in the performance of the Organisation’s functions; and
       (iv) whether reasonable attempts have been made to obtain the information or documents by other means; and
       (v) any submissions made by a Public Interest Advocate under section 180X; and
       (vi) any other matters the Minister considers relevant.

(3) A journalist information warrant issued under this section may specify conditions or restrictions relating to making authorisations under the authority of the warrant.

180M Issuing a journalist information warrant in an emergency

(1) The Director-General of Security may issue a journalist information warrant in relation to a particular person if:
   (a) a request under section 180J has been made for the issue of a journalist information warrant in relation to the particular person; and
   (b) the Minister has not, to the knowledge of the Director-General, made a decision under section 180L in relation to the request; and
   (c) within the preceding period of 3 months:
      (i) the Minister has not refused to issue a journalist information warrant in relation to the particular person; and
      (ii) the Director-General has not issued such a journalist information warrant; and
   (d) the Director-General is satisfied that, security will be, or is likely to be, seriously prejudiced if the access to which the request relates does not begin before a journalist information warrant can be issued and made available by the Minister; and
   (e) either:
      (i) the issuing of the warrant is authorised under subsection (3); or
      (ii) the Director-General is satisfied that none of the Ministers specified in subsection (4) is readily available or contactable.

(2) The Director-General must not issue a journalist information warrant unless the Director-General is satisfied as to the matters set out in paragraphs 180L(2)(a) and (b).
Authorisation to issue a warrant under this section

(3) A Minister specified in subsection (4) may, if he or she is satisfied as to the matters set out in paragraphs 180L(2)(a) and (b), orally give an authorisation under this subsection for the Director-General to issue the warrant under this section.

(4) The Ministers who may orally give an authorisation are:
   (a) the Minister; or
   (b) if the Director-General is satisfied that the Minister is not readily available or contactable—any of the following Ministers:
      (i) the Prime Minister;
      (ii) the Defence Minister;
      (iii) the Foreign Affairs Minister.

(5) The authorisation may specify conditions or restrictions relating to issuing the warrant.

(6) The Director-General must ensure that a written record of an authorisation given under subsection (3) is made as soon as practicable (but no later than 48 hours) after the authorisation is given.

Duration of a warrant under this section

(7) A journalist information warrant under this section must specify the period (not exceeding 48 hours) for which it is to remain in force. The Minister may revoke the warrant at any time before the end of the specified period.

Copies of warrant and other documents

(8) Immediately after issuing a journalist information warrant under this section, the Director-General must give the Minister:
   (a) a copy of the warrant; and
   (b) a statement of the grounds on which the warrant was issued; and
   (c) either:
      (i) a copy of the record made under subsection (6); or
      (ii) if the Director-General was satisfied as mentioned in subparagraph (1)(e)(ii)—a summary of the facts of the case justifying issuing the warrant.

(9) Within 3 business days after issuing a journalist information warrant under this section, the Director-General must give the Inspector-General of Intelligence and Security:
   (a) a copy of the warrant; and
   (b) either:
      (i) a copy of the record made under subsection (6); or
      (ii) if the Director-General was satisfied as mentioned in subparagraph (1)(e)(ii)—a summary of the facts of the case justifying issuing the warrant.

(10) Subsection (9) has effect despite subsection 185D(1).

180N Duration of a journalist information warrant

A journalist information warrant issued under section 180L must specify the period (not exceeding 6 months) for which it is to remain in force. The Minister may revoke the warrant at any time before the end of the specified period.
180P  Discontinuance of authorisations before expiry of a journalist information warrant

If, before a journalist information warrant issued under this Subdivision ceases to be in force, the Director-General of Security is satisfied that the grounds on which the warrant was issued have ceased to exist, he or she must:
(a) forthwith inform the Minister accordingly; and
(b) takes such steps as are necessary to ensure that the making of authorisations under the authority of the warrant is discontinued.

Subdivision C—Issuing journalist information warrants to enforcement agencies

180Q  Enforcement agency may apply for a journalist information warrant

(1) An enforcement agency may apply to a Part 4-1 issuing authority for a journalist information warrant in relation to a particular person.

(2) The application must be made on the agency’s behalf by:
   (a) if the agency is referred to in subsection 39(2)—a person referred to in that subsection in relation to that agency; or
   (b) otherwise:
      (i) the chief officer of the agency; or
      (ii) an officer of the agency (by whatever name called) who holds, or is acting in, an office or position in the agency nominated under subsection (3).

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

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

(5) The application may be made in writing or in any other form.

Note: The Electronic Transactions Act 1999 deals with giving information in writing by means of an electronic communication.

180R  Further information

(1) The Part 4-1 issuing authority may require:
   (a) in any case—the chief officer of the agency; or
   (b) if the application is made, on the agency’s behalf, by a person other than the chief officer—that other person;

   to give to the Part 4-1 issuing authority, within the period and in the form specified in the requirement, further information in connection with the application.

(2) If the chief officer or other person breaches the requirement, the Part 4-1 issuing authority may:
   (a) refuse to consider the application; or
   (b) refuse to take any action, or any further action, in relation to the application.

180S  Oaths and affirmations

(1) Information given to the Part 4-1 issuing authority in connection with the application must be verified on oath or affirmation.
For the purposes of this section, the Part 4-1 issuing authority may:

(a) administer an oath or affirmation; or
(b) authorise another person to administer an oath or affirmation.

The oath or affirmation may be administered in person, or by telephone, video call, video link or audio link.

**180T Issuing a journalist information warrant**

(1) After considering an application under section 180Q, the Part 4-1 issuing authority must:

(a) issue a journalist information warrant that authorises the making of authorisations under one or more of sections 178, 178A, 179 and 180 in relation to the particular person to which the application relates; or
(b) refuse to issue a journalist information warrant.

(2) The Part 4-1 issuing authority must not issue a journalist information warrant unless the Part 4-1 issuing authority is satisfied that:

(a) the warrant is reasonably necessary for whichever of the following purposes are applicable:
   (i) if the warrant would authorise the making of authorisations under section 178—for the enforcement of the criminal law;
   (ii) if the warrant would authorise the making of authorisations under section 178A—finding a person who the Australian Federal Police, or a Police Force of a State, has been notified is missing;
   (iii) if the warrant would authorise the making of authorisations under section 179—the enforcement of a law imposing a pecuniary penalty or for the protection of the public revenue;
   (iv) if the warrant would authorise the making of authorisations under section 180—the investigation of an offence of a kind referred to in subsection 180(4); and

(b) the public interest in issuing the warrant outweighs the public interest in protecting the confidentiality of the source in connection with whom authorisations would be made under the authority of the warrant, having regard to:
   (i) the extent to which the privacy of any person or persons would be likely to be interfered with by the disclosure of information or documents under authorisations that are likely to be made under the authority of the warrant; and
   (ii) the gravity of the matter in relation to which the warrant is sought; and
   (iii) the extent to which that information or those documents would be likely to assist in relation to that matter; and
   (iv) whether reasonable attempts have been made to obtain the information or documents by other means; and
   (v) any submissions made by a Public Interest Advocate under section 180X; and
   (vi) any other matters the Part 4-1 issuing authority considers relevant.

**180U Form and content of a journalist information warrant**

(1) A journalist information warrant issued under this Subdivision must be in accordance with the prescribed form and must be signed by the Part 4-1 issuing authority who issues it.

(2) A journalist information warrant issued under this Subdivision may specify conditions or restrictions relating to making authorisations under the authority of the warrant.
(3) A journalist information warrant issued under this Subdivision must specify, as the period for which it is to be in force, a period of up to 90 days.

(4) A Part 4-1 issuing authority must not vary a journalist information warrant issued under this Subdivision by extending the period for which it is to be in force.

(5) Neither of subsections (3) and (4) prevents the issue of a further warrant under this Act in relation to a person, in relation to which a warrant under this Act has, or warrants under this Act have, previously been issued.

180V Entry into force of a journalist information warrant

A journalist information warrant issued under this Subdivision comes into force when it is issued.

180W Revocation of a journalist information warrant by chief officer

(1) The chief officer of an enforcement agency:
   (a) may, at any time, by signed writing, revoke a journalist information warrant issued under this Subdivision to the agency; and
   (b) must do so, if he or she is satisfied that the grounds on which the warrant was issued to the agency have ceased to exist.

(2) The chief officer of an enforcement agency may delegate his or her power under paragraph (1)(a) to a certifying officer of the agency.

Subdivision D—Miscellaneous

180X Public Interest Advocates

(1) The Prime Minister shall declare, in writing, one or more persons to be Public Interest Advocates.

(2) A Public Interest Advocate may make submissions:
   (a) to the Minister about matters relevant to:
      (i) a decision to issue, or refuse to issue, a journalist information warrant under section 180L; or
      (ii) a decision about the conditions or restrictions (if any) that are to be specified in such a warrant; or
   (b) to a Part 4-1 issuing authority about matters relevant to:
      (i) a decision to issue, or refuse to issue, the warrant under section 180T; or
      (ii) a decision about the conditions or restrictions (if any) that are to be specified in such a warrant; or

(3) The regulations may prescribe matters relating to the performance of the role of a Public Interest Advocate.

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

(48) Schedule 1, page 17 (after proposed item 6L), at the end of Part 2, add:
6M After subparagraph 181A(3)(b)(i)
Insert:

(ia) to enable a person to comply with his or her obligations under section 185D or 185E; or

6N After paragraph 181A(3)(b)
Insert:

; or (c) the disclosure is:
    (i) to an IGIS official for the purpose of the Inspector-General of Intelligence and Security exercising powers, or performing functions or duties, under the Inspector-General of Intelligence and Security Act 1986; or
    (ii) by an IGIS official in connection with the IGIS official exercising powers, or performing functions or duties, under that Act.

6P After subparagraph 181A(6)(b)(i)
Insert:

(ia) to enable a person to comply with his or her obligations under section 185D or 185E; or

6Q After paragraph 181A(6)(b)
Insert:

; or (c) the use is by an IGIS official in connection with the IGIS official exercising powers, or performing functions or duties, under the Inspector-General of Intelligence and Security Act 1986.

[media sources; reports on access to data; IGIS]

(49) Schedule 1, page 17 (after proposed item 6Q), at the end of Part 2, add:

6R After subparagraph 181B(3)(b)(i)
Insert:

(ia) to enable a person to comply with his or her obligations under section 185D or 185E; or

6S Before subparagraph 181B(6)(b)(i)
Insert:

(ia) to enable a person to comply with his or her obligations under section 185D or 185E; or

[media sources; reports on access to data]

(50) Schedule 1, page 17 (after proposed item 6S), at the end of Part 2, add:

6T Subsection 182(2)
Repeal the subsection, substitute:

Exempt disclosures

(2) Paragraph (1)(b) does not apply to a disclosure of non-missing person information if:
    (a) the disclosure is reasonably necessary:
        (i) for a person to comply with his or her obligations under section 185D or 185E; or
(ii) for the performance by the Organisation of its functions; or
(iii) for the enforcement of the criminal law; or
(iv) for the enforcement of a law imposing a pecuniary penalty; or
(v) for the protection of the public revenue; or
(b) the disclosure is:
   (i) to an IGIS official for the purpose of the Inspector-General of Intelligence and
       Security exercising powers, or performing functions or duties, under the
       Inspector-General of Intelligence and Security Act 1986; or
   (ii) by an IGIS official in connection with the IGIS official exercising powers, or
       performing functions or duties, under that Act.

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

6U Subsection 182(3)

Repeal the subsection, substitute:

Exempt uses

(3) Paragraph (1)(b) does not apply to a use of non-missing person information if:
   (a) the use is reasonably necessary:
       (i) for a person to comply with his or her obligations under section 185D or 185E;
       or
       (ii) for the enforcement of the criminal law; or
       (iii) for the enforcement of a law imposing a pecuniary penalty; or
       (iv) for the protection of the public revenue; or
   (b) the use is by an IGIS official in connection with the IGIS official exercising powers,
       or performing functions or duties, under the Inspector-General of Intelligence and

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

[media sources; reports on access to data; IGIS]

(51) Schedule 1, page 17 (after proposed item 6U), at the end of Part 2, add:

6V At the end of Division 6 of Part 4-1

Add:

182A Disclosure/use offences: journalist information warrants

(1) A person commits an offence if:
   (a) the person discloses or uses information; and
   (b) the information is about any of the following:
       (i) whether a journalist information warrant (other than such a warrant that relates
           only to section 178A) has been, or is being, requested or applied for;
       (ii) the making of such a warrant;
       (iii) the existence or non-existence of such a warrant;
       (iv) the revocation of such a warrant.

Penalty: Imprisonment for 2 years.
(2) A person commits an offence if:
   (a) the person discloses or uses a document; and
   (b) the document consists (wholly or partly) of any of the following:
       (i) a journalist information warrant (other than such a warrant that relates only to
           section 178A);
       (ii) the revocation of such a warrant.

Penalty: Imprisonment for 2 years.

182B Permitted disclosure or use: journalist information warrants

Paragraphs 182A(1)(a) and (2)(a) do not apply to a disclosure or use of information or a
document if:
   (a) the disclosure or use is for the purposes of the warrant, revocation or notification
       concerned; or
   (b) the disclosure or use is reasonably necessary:
       (i) to enable the making of submissions under section 180X; or
       (ii) to enable a person to comply with his or her obligations under section 185D or
            185E; or
       (iii) to enable the Organisation to perform its functions; or
       (iv) to enforce the criminal law; or
       (v) to enforce a law imposing a pecuniary penalty; or
       (vi) to protect the public revenue; or
   (c) in the case of a disclosure—the disclosure is:
       (i) to an IGIS official for the purpose of the Inspector-General of Intelligence and
           Security exercising powers, or performing functions or duties, under the
           Inspector-General of Intelligence and Security Act 1986; or
       (ii) by an IGIS official in connection with the IGIS official exercising powers, or
            performing functions or duties, under that Act; or
   (d) in the case of a use—the use is by an IGIS official in connection with the IGIS
       official exercising powers, or performing functions or duties, under the
       Inspector-General of Intelligence and Security Act 1986.

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

(52) Schedule 1, page 17 (after proposed item 6V), at the end of Part 2, add:

6W At the end of section 185

Add:

(3) This section does not limit subsection 187N(3).

(53) Schedule 1, page 17 (after proposed item 6W), at the end of Part 2, add:

6X After section 185C

Insert:
185D Notification etc. of authorisations intended to identify media sources

The Organisation

(1) If a journalist information warrant is issued under Subdivision B of Division 4C of Part 4-1:
   (a) the Director-General of Security must, as soon as practicable, give a copy of the warrant to the Inspector-General of Intelligence and Security; and
   (b) the Minister must, as soon as practicable, cause the Parliamentary Joint Committee on Intelligence and Security to be notified of the issuing of the warrant.

(2) If an authorisation under Division 3 of Part 4-1 is made under the authority of the warrant, the Director-General of Security must, as soon as practicable after the expiry of the warrant, give a copy of the authorisation to the Inspector-General of Intelligence and Security.

(3) If:
   (a) the Inspector-General gives to the Minister a report under section 22 or 25A of the Inspector-General of Intelligence and Security Act 1986; and
   (b) the report relates (wholly or partly) to one or both of the following:
       (i) a journalist information warrant issued to the Organisation;
       (ii) one or more authorisations referred to in subsection (2) of this section;
   the Minister must, as soon as practicable, cause a copy of the report to be given to the Parliamentary Joint Committee on Intelligence and Security.

(4) The Parliamentary Joint Committee on Intelligence and Security may request a briefing from the Inspector-General on:
   (a) a journalist information warrant; or
   (b) an authorisation or authorisations;
   to which a report referred to in paragraph (3)(b) of this section relates.

Enforcement agencies

(5) If a journalist information warrant is issued to an enforcement agency:
   (a) if the agency was the Australian Federal Police:
       (i) the Commissioner of Police must, as soon as practicable, give copies of the warrant to the Minister and the Ombudsman; and
       (ii) the Minister must, as soon as practicable after receiving a copy, cause the Parliamentary Joint Committee on Intelligence and Security to be notified of the issuing of the warrant; and
   (b) otherwise—the chief officer of the agency must, as soon as practicable, give a copy of the warrant to the Ombudsman.

(6) If an authorisation under Division 4 of Part 4-1 is made under the authority of the warrant, the chief officer of the agency must, as soon as practicable after the expiry of the warrant, give a copy of the authorisation to the Ombudsman.

(7) If:
   (a) the Ombudsman gives to the Minister a report under section 186J of this Act; and
   (b) the report relates (wholly or partly) to one or both of the following:
       (i) a journalist information warrant issued to the Australian Federal Police;
one or more authorisations, referred to in subsection (6) of this section, that were made by one or more authorised officers of the Australian Federal Police; the Minister must, as soon as practicable, cause a copy of the report to be given to the Parliamentary Joint Committee on Intelligence and Security.

(8) The Parliamentary Joint Committee on Intelligence and Security may request a briefing from the Ombudsman on:
   (a) a journalist information warrant; or
   (b) an authorisation or authorisations;
   to which a report referred to in paragraph (7)(b) of this section relates.

185E Reports on access to retained data

The Organisation

(1) If:
   (a) the Inspector-General of Intelligence and Security gives to the Minister a report under section 22 or 25A of the Inspector-General of Intelligence and Security Act 1986; and
   (b) the report relates (wholly or partly) to the purpose or manner of access to retained data by means of one or more authorisations under Division 3 of Part 4-1 of this Act;
   the Minister must, as soon as practicable, cause a copy of the report to be given to the Parliamentary Joint Committee on Intelligence and Security.

(2) The Parliamentary Joint Committee on Intelligence and Security may request a briefing from the Inspector-General on the authorisation or authorisations.

Australian Federal Police

(3) If:
   (a) the Ombudsman gives to the Minister a report under section 186J of this Act; and
   (b) the report relates (wholly or partly) to the purpose or manner of access to retained data by means of one or more authorisations under Division 4 or 4A of Part 4-1 of this Act; and
   (c) the authorisation or authorisations were made by one or more authorised officers of the Australian Federal Police;
   the Minister must, as soon as practicable, cause a copy of the report to be given to the Parliamentary Joint Committee on Intelligence and Security.

(4) The Parliamentary Joint Committee on Intelligence and Security may request a briefing from the Ombudsman on the authorisation or authorisations.

6Y At the end of subsection 186(1)

Add:
; and (e) the offences and other matters for which authorised officers of the agency made authorisations under sections 178, 178A, 179 and 180 during that year; and
(f) the lengths of time for which the information or documents that were covered by those authorisations had been held when the authorisations were made; and

(54) Schedule 1, page 17 (after proposed item 6X), at the end of Part 2, add:
(g) the number of occasions during that year on which authorised officers of the agency made authorisations relating to retained data that included information of a kind referred to in item 1 of the table in subsection 187AA(1); and

(h) the number of occasions during that year on which authorised officers of the agency made authorisations relating to retained data that included information of a kind referred to in item 2, 3, 4, 5 or 6 of the table in subsection 187AA(1); and

(i) the number of authorisations, referred to in paragraph (e) of this subsection, that were made under journalist information warrants issued to the agency under Subdivision C of Division 4C of Part 4-1 of that Act; and

(j) the number of journalist information warrants issued to the agency under that Subdivision during the period; and

(k) information of a kind declared under subsection (1E) of this section.

6Z After subsection 186(1)

Insert:

(1A) The report under subsection (1) is to set out the offences and other matters referred to in paragraph (1)(e) by means of the categories declared under subsection (1B).

(1B) The Minister may, by legislative instrument, declare categories of offences and other matters into which the offences and other matters are to be divided for the purposes of paragraph (1)(e).

(1C) The report under subsection (1) is to set out the matters referred to in paragraph (1)(f) by specifying:

(a) in relation to each of 8 successive periods of 3 months, the number of the authorisations made for information or documents held for lengths of time included in that period; and

(b) the number of the authorisations made for information or documents held for lengths of time exceeding 24 months.

(1D) For the purposes of paragraph (1)(f), disregard any authorisations under subsection 180(2), except to the extent that they include authorisations under subsection 180(3).

(1E) The Minister may, by legislative instrument, declare kinds of information that are to be set out in the report under subsection (1).

[information on authorisations and retained data]

(55) Schedule 1, item 9, page 19 (line 3), after “187K(1)”, insert “or 187KA(2)”.

[review by the ACMA]

(56) Schedule 1, item 10, page 19 (line 11), omit “or 187K”, substitute “, 187K or 187KA”.

[review by the ACMA]

(57) Schedule 1, page 20 (after line 7), at the end of Part 3, add:

12 First reporting period after commencement of Part 5-1A

(1) The annual report referred to in subsection 94(1) of the Australian Security Intelligence Organisation Act 1979 for the period during which Part 5-1A commenced is to include a statement of the matters referred to in paragraphs 94(2A)(c) to (j) of that Act as amended by
this Act only to the extent that the matters relate to the part of that period occurring after Part 5-1A commenced.

(2) A report under section 186 of the Telecommunications (Interception and Access) Act 1979 as amended by this Act for the period during which Part 5-1A commenced is to include a statement of the matters referred to in paragraphs 186(1)(e) to (k) of that Act as so amended only to the extent that the matters relate to the part of that period occurring after Part 5-1A commenced.

(3) In this item:

Part 5-1A means Part 5-1A of the Telecommunications (Interception and Access) Act 1979 as amended by this Act.

[first reporting periods]

(58) Schedule 2, item 3, page 21 (after line 20), after paragraph 110A(1)(e), insert:

(a) the Australian Securities and Investments Commission;
(b) the Australian Competition and Consumer Commission;

[criminal law-enforcement agencies]

(59) Schedule 2, item 3, page 22 (line 5), omit “the”, substitute “an”.

[request for declaration not required]

(60) Schedule 2, item 3, page 22 (after line 9), after subsection 110A(3), insert:

(3A) The Minister may make the declaration whether or not the head of the authority or body has made a request under subsection (2).

(3B) The Minister must not make the declaration unless the Minister is satisfied on reasonable grounds that the functions of the authority or body include investigating serious contraventions.

[request for declaration not required; Minister must be satisfied as to functions]

(61) Schedule 2, item 3, page 22 (lines 12 and 13), omit paragraph 110A(4)(a).

[Minister must be satisfied as to functions]

(62) Schedule 2, item 3, page 22 (line 16), omit “those”.

[Minister must be satisfied as to functions]

(63) Schedule 2, item 3, page 22 (lines 21 to 24), omit subparagraph 110A(4)(c)(ii), substitute:

(ii) is required to comply with a binding scheme that provides protection of personal information that meets the requirements of subsection (4A); or

[privacy protection schemes]

(64) Schedule 2, item 3, page 22 (line 26), omit “a level of”.

[privacy protection schemes]

(65) Schedule 2, item 3, page 22 (after line 37), after subsection 110A(4), insert:

(4A) For the purposes of subparagraphs (4)(c)(ii) and (iii), the protection of personal information provided by the scheme must:

(a) be comparable to the protection provided by the Australian Privacy Principles; and
(b) include a mechanism for monitoring the authority’s or body’s compliance with the scheme; and
(c) include a mechanism that enables an individual to seek recourse if his or her personal information is mishandled.  

[privacy protection schemes]

(66) Schedule 2, item 3, page 23 (after line 28), at the end of section 110A, add:

(10) A declaration under subsection (3):
   (a) comes into force when it is made, or on such later day as is specified in the declaration; and
   (b) ceases to be in force at the end of the period of 40 sitting days of a House of the Parliament after the declaration comes into force.

(11) If a Bill is introduced into either House of the Parliament that includes an amendment of subsection (1), the Minister:
   (a) must refer the amendment to the Parliamentary Joint Committee on Intelligence and Security for review; and
   (b) must not in that referral specify, as the period within which the Committee is to report on its review, a period that will end earlier than 15 sitting days of a House of the Parliament after the introduction of the Bill.

[declarations ceasing to be in force]

(67) Schedule 2, item 4, page 24 (line 8), omit “the”, substitute “an”.

[request for declaration not required]

(68) Schedule 2, item 4, page 24 (after line 11), after subsection 176A(3), insert:

(3A) The Minister may make the declaration whether or not the head of the authority or body has made a request under subsection (2).

(3B) The Minister must not make the declaration unless the Minister is satisfied on reasonable grounds that the functions of the authority or body include:
   (a) enforcement of the criminal law; or
   (b) administering a law imposing a pecuniary penalty; or
   (c) administering a law relating to the protection of the public revenue.

[request for declaration not required; Minister must be satisfied as to functions]

(69) Schedule 2, item 4, page 24 (lines 14 to 18), omit paragraph 176A(4)(a).

[Minister must be satisfied as to functions]

(70) Schedule 2, item 4, page 24 (line 21), omit “those functions”, substitute “the functions referred to in subsection (3B)”.

[Minister must be satisfied as to functions]

(71) Schedule 2, item 4, page 24 (lines 25 to 28), omit subparagraph 176A(4)(c)(ii), substitute:
   (ii) is required to comply with a binding scheme that provides protection of personal information that meets the requirements of subsection (4A); or

[privacy protection schemes]

(72) Schedule 2, item 4, page 24 (line 30), omit “a level of”.

[privacy protection schemes]

(73) Schedule 2, item 4, page 25 (after line 3), after subsection 176A(4), insert:
(4A) For the purposes of subparagraphs (4)(c)(ii) and (iii), the protection of personal information provided by the scheme must:
(a) be comparable to the protection provided by the Australian Privacy Principles; and
(b) include a mechanism for monitoring the authority’s or body’s compliance with the scheme; and
(c) include a mechanism that enables an individual to seek recourse if his or her personal information is mishandled.

[privacy protection schemes]

(74) Schedule 2, item 4, page 25 (after line 22), at the end of section 176A, add:

(10) A declaration under subsection (3):
(a) comes into force when it is made, or on such later day as is specified in the declaration; and
(b) ceases to be in force at the end of the period of 40 sitting days of a House of the Parliament after the declaration comes into force.

(11) If a Bill is introduced into either House of the Parliament that includes an amendment of subsection (1), the Minister:
(a) must refer the amendment to the Parliamentary Joint Committee on Intelligence and Security for review; and
(b) must not in that referral specify, as the period within which the Committee is to report on its review, a period that will end earlier than 15 sitting days of a House of the Parliament after the introduction of the Bill.

[declarations ceasing to be in force]