

2016-2017-2018

The Parliament of the
Commonwealth of Australia

HOUSE OF REPRESENTATIVES

As passed by both Houses

**Telecommunications and Other
Legislation Amendment (Assistance and
Access) Bill 2018**

No. , 2018

**A Bill for an Act to amend the law relating to
telecommunications, computer access warrants and
search warrants, and for other purposes**

Contents

1	Short title.....	1
2	Commencement.....	1
3	Schedules.....	3
Schedule 1—Industry assistance		4
Part 1—Amendments		4
<i>Administrative Decisions (Judicial Review) Act 1977</i>		4
<i>Australian Security Intelligence Organisation Act 1979</i>		4
<i>Criminal Code Act 1995</i>		5
<i>Independent National Security Legislation Monitor Act 2010</i>		5
<i>Telecommunications Act 1997</i>		6
<i>Telecommunications (Interception and Access) Act 1979</i>		107
Part 2—Amendments contingent on the commencement of the Federal Circuit and Family Court of Australia Act 2018		109
<i>Telecommunications Act 1997</i>		109
Schedule 2—Computer access warrants etc.		110
Part 1—Amendments		110
<i>Australian Security Intelligence Organisation Act 1979</i>		110
<i>Mutual Assistance in Criminal Matters Act 1987</i>		119
<i>Surveillance Devices Act 2004</i>		121
<i>Telecommunications Act 1997</i>		176
<i>Telecommunications (Interception and Access) Act 1979</i>		177
Part 2—Application provisions		188
Part 3—Amendments contingent on the commencement of the Crimes Legislation Amendment (International Crime Cooperation and Other Measures) Act 2018		189
<i>International Criminal Court Act 2002</i>		189
<i>International War Crimes Tribunals Act 1995</i>		190
<i>Surveillance Devices Act 2004</i>		191

Schedule 3—Search warrants issued under the Crimes Act 1914	195
<i>Crimes Act 1914</i>	195
Schedule 4—Search warrants issued under the Customs Act 1901	205
<i>Customs Act 1901</i>	205
Schedule 5—Australian Security Intelligence Organisation	217
<i>Australian Security Intelligence Organisation Act 1979</i>	217

1 **A Bill for an Act to amend the law relating to**
2 **telecommunications, computer access warrants and**
3 **search warrants, and for other purposes**

4 The Parliament of Australia enacts:

5 **1 Short title**

6 This Act is the *Telecommunications and Other Legislation*
7 *Amendment (Assistance and Access) Act 2018.*

8 **2 Commencement**

9 (1) Each provision of this Act specified in column 1 of the table
10 commences, or is taken to have commenced, in accordance with
11 column 2 of the table. Any other statement in column 2 has effect
12 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, Part 1	The day after this Act receives the Royal Assent.	
3. Schedule 1, Part 2	The later of: (a) immediately after the commencement of Part 1 of Schedule 1 to this Act; and (b) immediately after the commencement of section 3 of the <i>Federal Circuit and Family Court of Australia Act 2018</i> . However, the provisions do not commence at all if the event mentioned in paragraph (b) does not occur.	
4. Schedule 2, Parts 1 and 2	The day after this Act receives the Royal Assent.	
5. Schedule 2, Part 3	The later of: (a) immediately after the commencement of Part 1 of Schedule 2 to this Act; and (b) immediately after the commencement of Part 6 of Schedule 1 to the <i>Crimes Legislation Amendment (International Crime Cooperation and Other Measures) Act 2018</i> . However, the provisions do not commence at all if the event mentioned in paragraph (b) does not occur.	
6. Schedules 3, 4 and 5	The day after this Act receives the Royal Assent.	
	Note:	This table relates only to the provisions of this Act as originally enacted. It will not be amended to deal with any later amendments of this Act.

1 (2) Any information in column 3 of the table is not part of this Act.
2 Information may be inserted in this column, or information in it
3 may be edited, in any published version of this Act.

4 **3 Schedules**

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

1 **Schedule 1—Industry assistance**

2 **Part 1—Amendments**

3 *Administrative Decisions (Judicial Review) Act 1977*

4 **1 After paragraph (daaa) of Schedule 1**

5 Insert:

6 (daaaa) decisions under Part 15 of the *Telecommunications Act 1997*;

7 *Australian Security Intelligence Organisation Act 1979*

8 **1A After subsection 94(2B)**

9 Insert:

10 (2BA) A report under subsection (1) must also include a statement of:

- 11 (a) the total number of technical assistance requests given by the
12 Director-General under paragraph 317G(1)(a) of the
13 *Telecommunications Act 1997* during the period; and
14 (b) the total number of technical assistance notices given by the
15 Director-General under section 317L of the
16 *Telecommunications Act 1997* during the period; and
17 (c) the total number of technical capability notices given by the
18 Attorney-General under section 317T of the
19 *Telecommunications Act 1997* during the period that relate to
20 the Organisation.

21 (2BB) For the purposes of paragraph (2BA)(c), a technical capability
22 notice *relates to* the Organisation if the acts or things specified in
23 the notice:

- 24 (a) are directed towards ensuring that a designated
25 communications provider (within the meaning of Part 15 of
26 the *Telecommunications Act 1997*) is capable of giving listed
27 help (within the meaning of section 317T of that Act) to the
28 Organisation in relation to a matter covered by
29 paragraph 317T(2)(a) of that Act; or

1 (b) are by way of giving help to the Organisation in relation to a
2 matter covered by paragraph 317T(2)(b) of the
3 *Telecommunications Act 1997*.

4 ***Criminal Code Act 1995***

5 **2 After subsection 474.6(7) of the *Criminal Code***

6 Insert:

7 (7A) A person is not criminally responsible for an offence against
8 subsection (5) if the conduct of the person:

- 9 (a) is in accordance with a technical assistance request; or
10 (b) is in compliance with a technical assistance notice; or
11 (c) is in compliance with a technical capability notice.

12 **3 After subparagraph 476.2(4)(b)(iii) of the *Criminal Code***

13 Insert:

- 14 or (iv) in accordance with a technical assistance request; or
15 (v) in compliance with a technical assistance notice; or
16 (vi) in compliance with a technical capability notice;

17 **4 Dictionary in the *Criminal Code***

18 Insert:

19 ***technical assistance notice*** has the same meaning as in Part 15 of
20 the *Telecommunications Act 1997*.

21 ***technical assistance request*** has the same meaning as in Part 15 of
22 the *Telecommunications Act 1997*.

23 ***technical capability notice*** has the same meaning as in Part 15 of
24 the *Telecommunications Act 1997*.

25 ***Independent National Security Legislation Monitor Act 2010***

26 **4A At the end of subsection 6(1)**

27 Add:

28 ; (e) the function conferred by subsection (1D).

1 **4B Before subsection 6(2)**

2 Insert:

3 (1D) The Independent National Security Legislation Monitor must:

- 4 (a) review the operation, effectiveness and implications of the
5 amendments made by the *Telecommunications and Other*
6 *Legislation Amendment (Assistance and Access) Act 2018*;
7 and
8 (b) do so as soon as practicable after the 18-month period
9 beginning on the day that Act receives the Royal Assent.

10 ***Telecommunications Act 1997***

11 **5 Section 7**

12 Insert:

13 *ASIO* means the Australian Security Intelligence Organisation.

14 **6 Section 7 (paragraph (a) of the definition of *civil penalty***
15 ***provision*)**

16 After “this Act” (first occurring), insert “(other than section 317ZB)”.

17 **7 After Part 14**

18 Insert:

19 **Part 15—Industry assistance**

20 **Division 1—Introduction**

21 **317A Simplified outline of this Part**

- 22
- 23
- 24
- 25
- 26
- The Director-General of Security, the Director-General of the Australian Secret Intelligence Service, the Director-General of the Australian Signals Directorate or the chief officer of an interception agency may give a technical assistance request to a designated communications provider.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37

- A technical assistance request may ask the provider to do acts or things on a voluntary basis that are directed towards ensuring that the provider is capable of giving certain types of help to ASIO, the Australian Secret Intelligence Service, the Australian Signals Directorate or an interception agency in relation to:
 - (a) in the case of ASIO—safeguarding national security; or
 - (b) in the case of the Australian Secret Intelligence Service—the interests of Australia’s national security, the interests of Australia’s foreign relations or the interests of Australia’s national economic well-being; or
 - (c) in the case of the Australian Signals Directorate—providing material, advice and other assistance on matters relating to the security and integrity of information that is processed, stored or communicated by electronic or similar means; or
 - (d) in the case of an interception agency—enforcing the criminal law, so far as it relates to serious Australian offences; or
 - (e) in the case of an interception agency—assisting the enforcement of the criminal laws in force in a foreign country, so far as those laws relate to serious foreign offences.

- A technical assistance request may ask the provider to give help to ASIO, the Australian Secret Intelligence Service, the Australian Signals Directorate or an interception agency on a voluntary basis in relation to:
 - (a) in the case of ASIO—safeguarding national security; or
 - (b) in the case of the Australian Secret Intelligence Service—the interests of Australia’s national security, the interests of Australia’s foreign relations or the interests of Australia’s national economic well-being; or
 - (c) in the case of the Australian Signals Directorate—providing material, advice and other assistance on matters relating to the security and integrity of information that is processed, stored or communicated by electronic or similar means; or

1
2
3
4
5
6
7

8
9
10
11
12
13
14
15
16
17
18

19
20

21
22
23
24
25
26
27
28
29
30

31
32
33
34
35

- (d) in the case of an interception agency—enforcing the criminal law, so far as it relates to serious Australian offences; or
 - (e) in the case of an interception agency—assisting the enforcement of the criminal laws in force in a foreign country, so far as those laws relate to serious foreign offences.
- The Director-General of Security or the chief officer of an interception agency may give a designated communications provider a notice, to be known as a technical assistance notice, that requires the provider to do acts or things by way of giving certain types of help to ASIO or the agency in relation to:
 - (a) enforcing the criminal law, so far as it relates to serious Australian offences; or
 - (b) assisting the enforcement of the criminal laws in force in a foreign country, so far as those laws relate to serious foreign offences; or
 - (c) safeguarding national security.
 - The Attorney-General may give a designated communications provider a notice, to be known as a technical capability notice.
 - A technical capability notice may require the provider to do acts or things directed towards ensuring that the provider is capable of giving certain types of help to ASIO or an interception agency in relation to:
 - (a) enforcing the criminal law, so far as it relates to serious Australian offences; or
 - (b) assisting the enforcement of the criminal laws in force in a foreign country, so far as those laws relate to serious foreign offences; or
 - (c) safeguarding national security.
 - A technical capability notice may require the provider to do acts or things by way of giving certain types of help to ASIO or an interception agency in relation to:
 - (a) enforcing the criminal law, so far as it relates to serious Australian offences; or

- 1 (b) assisting the enforcement of the criminal laws in force in
2 a foreign country, so far as those laws relate to serious
3 foreign offences; or
4 (c) safeguarding national security.

5 **317B Definitions**

6 In this Part:

7 ***access***, when used in relation to material, includes:

- 8 (a) access that is subject to a pre-condition (for example, the use
9 of a password); and
10 (b) access by way of push technology; and
11 (c) access by way of a standing request.

12 ***ASIO affiliate*** has the same meaning as in the *Australian Security*
13 *Intelligence Organisation Act 1979*.

14 ***ASIO employee*** has the same meaning as in the *Australian Security*
15 *Intelligence Organisation Act 1979*.

16 ***chief officer*** of an interception agency has the meaning given by
17 section 317ZM.

18 ***contracted service provider***, in relation to a designated
19 communications provider, means a person who performs services
20 for or on behalf of the provider, but does not include a person who
21 performs such services in the capacity of an employee of the
22 provider.

23 ***designated communications provider*** has the meaning given by
24 section 317C.

25 ***electronic protection*** includes:

- 26 (a) authentication; and
27 (b) encryption.

28 ***electronic service*** has the meaning given by section 317D.

29 ***eligible activities*** of a designated communications provider has the
30 meaning given by section 317C.

1 **entrusted ASD person** means a person who:
2 (a) is a staff member of the Australian Signals Directorate; or
3 (b) has entered into a contract, agreement or arrangement with
4 the Australian Signals Directorate; or
5 (c) is an employee or agent of a person who has entered into a
6 contract, agreement or arrangement with the Australian
7 Signals Directorate.

8 **entrusted ASIO person** means an entrusted person (within the
9 meaning of the *Australian Security Intelligence Organisation Act*
10 *1979*).

11 **entrusted ASIS person** means a person who:
12 (a) is a staff member or agent of the Australian Secret
13 Intelligence Service; or
14 (b) has entered into a contract, agreement or arrangement with
15 the Australian Secret Intelligence Service; or
16 (c) is an employee or agent of a person who has entered into a
17 contract, agreement or arrangement with the Australian
18 Secret Intelligence Service.

19 **giving help:**
20 (a) when used in relation to ASIO—includes giving help to an
21 ASIO employee or an ASIO affiliate; or
22 (b) when used in relation to the Australian Secret Intelligence
23 Service—includes giving help to a staff member of the
24 Australian Secret Intelligence Service; or
25 (c) when used in relation to the Australian Signals Directorate—
26 includes giving help to a staff member of the Australian
27 Signals Directorate; or
28 (d) when used in relation to an interception agency—includes
29 giving help to an officer of the agency.

30 **Home Affairs Minister** means the Minister administering the
31 *Telecommunications (Interception and Access) Act 1979*.

32 **IGIS official** has the same meaning as in the *Australian Security*
33 *Intelligence Organisation Act 1979*.

34 **interception agency** means:

- 1 (a) the Australian Federal Police; or
2 (b) the Australian Crime Commission; or
3 (c) the Police Force of a State or the Northern Territory.

4 **listed act or thing** has the meaning given by section 317E.

5 **material** means material:

- 6 (a) whether in the form of text; or
7 (b) whether in the form of data; or
8 (c) whether in the form of speech, music or other sounds; or
9 (d) whether in the form of visual images (moving or otherwise);
10 or
11 (e) whether in any other form; or
12 (f) whether in any combination of forms.

13 **officer** of an interception agency has the meaning given by
14 section 317ZM.

15 **Ombudsman official** means:

- 16 (a) the Commonwealth Ombudsman; or
17 (b) a Deputy Commonwealth Ombudsman; or
18 (c) a person who is a member of the staff referred to in
19 subsection 31(1) of the *Ombudsman Act 1976*.

20 **serious Australian offence** means an offence against a law of the
21 Commonwealth, a State or a Territory that is punishable by a
22 maximum term of imprisonment of 3 years or more or for life.

23 **serious foreign offence** means an offence against a law in force in
24 a foreign country that is punishable by a maximum term of
25 imprisonment of 3 years or more or for life.

26 **staff member**, when used in relation to the Australian Secret
27 Intelligence Service or the Australian Signals Directorate, has the
28 same meaning as in the *Intelligence Services Act 2001*.

29 **State or Territory inspecting authority**, in relation to an
30 interception agency of a State or Territory, means the authority
31 that, under the law of the State or Territory concerned, has the
32 function of making inspections of a similar kind to those provided
33 for in section 55 of the *Surveillance Devices Act 2004* when the

1 interception agency is exercising powers under the law of that State
2 or Territory that is of a similar nature to that Act.

3 **supply:**

- 4 (a) when used in relation to:
5 (i) a facility; or
6 (ii) customer equipment; or
7 (iii) a component;
8 includes supply (including re-supply) by way of sale,
9 exchange, lease, hire or hire-purchase; and
10 (b) when used in relation to software—includes provide, grant or
11 confer rights, privileges or benefits.

12 **systemic vulnerability** means a vulnerability that affects a whole
13 class of technology, but does not include a vulnerability that is
14 selectively introduced to one or more target technologies that are
15 connected with a particular person. For this purpose, it is
16 immaterial whether the person can be identified.

17 **systemic weakness** means a weakness that affects a whole class of
18 technology, but does not include a weakness that is selectively
19 introduced to one or more target technologies that are connected
20 with a particular person. For this purpose, it is immaterial whether
21 the person can be identified.

22 **target technology:**

- 23 (a) for the purposes of this Part, a particular carriage service, so
24 far as the service is used, or is likely to be used, (whether
25 directly or indirectly) by a particular person, is a **target**
26 **technology** that is connected with that person; and
27 (b) for the purposes of this Part, a particular electronic service,
28 so far as the service is used, or is likely to be used, (whether
29 directly or indirectly) by a particular person, is a **target**
30 **technology** that is connected with that person; and
31 (c) for the purposes of this Part, particular software installed, or
32 to be installed, on:
33 (i) a particular computer; or
34 (ii) a particular item of equipment;

- 1 used, or likely to be used, (whether directly or indirectly) by
2 a particular person is a **target technology** that is connected
3 with that person; and
- 4 (d) for the purposes of this Part, a particular update of software
5 that has been installed on:
- 6 (i) a particular computer; or
7 (ii) a particular item of equipment;
- 8 used, or likely to be used, (whether directly or indirectly) by
9 a particular person is a **target technology** that is connected
10 with that person; and
- 11 (e) for the purposes of this Part, a particular item of customer
12 equipment used, or likely to be used, (whether directly or
13 indirectly) by a particular person is a **target technology** that
14 is connected with that person; and
- 15 (f) for the purposes of this Part, a particular data processing
16 device used, or likely to be used, (whether directly or
17 indirectly) by a particular person is a **target technology** that
18 is connected with that person.

19 For the purposes of paragraphs (a), (b), (c), (d), (e) and (f), it is
20 immaterial whether the person can be identified.

21 **technical assistance notice** means a notice given under
22 section 317L.

23 **technical assistance notice information** means:

- 24 (a) information about any of the following:
- 25 (i) the giving of a technical assistance notice;
- 26 (ia) consultation relating to the giving of a technical
27 assistance notice;
- 28 (ii) the existence or non-existence of a technical assistance
29 notice;
- 30 (iii) the variation of a technical assistance notice;
- 31 (iv) the revocation of a technical assistance notice;
- 32 (v) the requirements imposed by a technical assistance
33 notice;
- 34 (vi) any act or thing done in compliance with a technical
35 assistance notice; or
- 36 (b) any other information about a technical assistance notice.

1 **technical assistance request** means a request under
2 paragraph 317G(1)(a).

3 **technical assistance request information** means:

- 4 (a) information about any of the following:
- 5 (i) the giving of a technical assistance request;
 - 6 (ii) the existence or non-existence of a technical assistance
7 request;
 - 8 (iii) the acts or things covered by a technical assistance
9 request;
 - 10 (iv) any act or thing done in accordance with a technical
11 assistance request; or
- 12 (b) any other information about a technical assistance request.

13 **technical capability notice** means a notice given under
14 section 317T.

15 **technical capability notice information** means:

- 16 (a) information about any of the following:
- 17 (i) the giving of a technical capability notice;
 - 18 (ii) consultation relating to the giving of a technical
19 capability notice;
 - 20 (iii) the existence or non-existence of a technical capability
21 notice;
 - 22 (iv) the variation of a technical capability notice;
 - 23 (iva) consultation relating to the variation of a technical
24 capability notice;
 - 25 (v) the revocation of a technical capability notice;
 - 26 (vi) the requirements imposed by a technical capability
27 notice;
 - 28 (vii) any act or thing done in compliance with a technical
29 capability notice; or
- 30 (b) any other information about a technical capability notice.

31 **317C Designated communications provider etc.**

32 For the purposes of this Part, the following table defines:

- 33 (a) **designated communications provider**; and
-

1 (b) the *eligible activities* of a designated communications
2 provider.
3

Designated communications provider and eligible activities

Item	A person is a designated communications provider if and the eligible activities of the person are ...
1	the person is a carrier or carriage service provider	(a) the operation by the person of telecommunications networks, or facilities, in Australia; or (b) the supply by the person of listed carriage services
2	the person is a carriage service intermediary who arranges for the supply by a carriage service provider of listed carriage services	(a) the arranging by the person for the supply by the carriage service provider of listed carriage services; or (b) the operation by the carriage service provider of telecommunications networks, or facilities, in Australia; or (c) the supply by the carriage service provider of listed carriage services
3	the person provides a service that facilitates, or is ancillary or incidental to, the supply of a listed carriage service	the provision by the person of a service that facilitates, or is ancillary or incidental to, the supply of a listed carriage service
4	the person provides an electronic service that has one or more end-users in Australia	the provision by the person of an electronic service that has one or more end-users in Australia
5	the person provides a service that facilitates, or is ancillary or incidental to, the provision of an electronic service that has one or more end-users in Australia	the provision by the person of a service that facilitates, or is ancillary or incidental to, the provision of an electronic service that has one or more end-users in Australia
6	the person develops, supplies or updates software used, for use, or likely to be used, in connection with: (a) a listed carriage service; or (b) an electronic service that has one	(a) the development by the person of any such software; or (b) the supply by the person of any such software; or (c) the updating by the person of any such software

Schedule 1 Industry assistance
Part 1 Amendments

Designated communications provider and eligible activities		
Item	A person is a designated communications provider if and the eligible activities of the person are ...
	or more end-users in Australia	
7	the person manufactures, supplies, installs, maintains or operates a facility	(a) the manufacture by the person of a facility for use, or likely to be used, in Australia; or (b) the supply by the person of a facility for use, or likely to be used, in Australia; or (c) the installation by the person of a facility in Australia; or (d) the maintenance by the person of a facility in Australia; or (e) the operation by the person of a facility in Australia
8	the person manufactures or supplies components for use, or likely to be used, in the manufacture of a facility for use, or likely to be used, in Australia	(a) the manufacture by the person of any such components; or (b) the supply by the person of any such components
9	the person connects a facility to a telecommunications network in Australia	the connection by the person of a facility to a telecommunications network in Australia
10	the person manufactures or supplies customer equipment for use, or likely to be used, in Australia	(a) the manufacture by the person of any such customer equipment; or (b) the supply by the person of any such customer equipment
11	the person manufactures or supplies components for use, or likely to be used, in the manufacture of customer equipment for use, or likely to be used, in Australia	(a) the manufacture by the person of any such components; or (b) the supply by the person of any such components
12	the person: (a) installs or maintains customer equipment in Australia; and (b) does so otherwise than in the capacity of end-user of the equipment	(a) any such installation by the person of customer equipment; or (b) any such maintenance by the person of customer equipment

Designated communications provider and eligible activities

Item	A person is a designated communications provider if and the eligible activities of the person are ...
13	the person: (a) connects customer equipment to a telecommunications network in Australia; and (b) does so otherwise than in the capacity of end-user of the equipment	any such connection by the person of customer equipment to a telecommunications network in Australia
14	the person is a constitutional corporation who: (a) manufactures; or (b) supplies; or (c) installs; or (d) maintains; data processing devices	(a) the manufacture by the person of data processing devices for use, or likely to be used, in Australia; or (b) the supply by the person of data processing devices for use, or likely to be used, in Australia; or (c) the installation by the person of data processing devices in Australia; or (d) the maintenance by the person of data processing devices in Australia
15	the person is a constitutional corporation who: (a) develops; or (b) supplies; or (c) updates; software that is capable of being installed on a computer, or other equipment, that is, or is likely to be, connected to a telecommunications network in Australia	(a) the development by the person of any such software; or (b) the supply by the person of any such software; or (c) the updating by the person of any such software
1	Note 1:	See also sections 317HAA, 317MAA and 317TAA (provision of advice to designated communications providers).
2		
3	Note 2:	See also section 317ZT (alternative constitutional basis).

1 **317D Electronic service**

2 (1) For the purposes of this Part, *electronic service* means:

3 (a) a service that allows end-users to access material using a
4 carriage service; or

5 (b) a service that delivers material to persons having equipment
6 appropriate for receiving that material, where the delivery of
7 the service is by means of a carriage service;

8 but does not include:

9 (c) a broadcasting service; or

10 (d) a datacasting service (within the meaning of the
11 *Broadcasting Services Act 1992*).

12 (2) For the purposes of subsection (1), *service* includes a website.

13 (3) For the purposes of this Part, a person does not provide an
14 electronic service merely because the person supplies a carriage
15 service that enables material to be accessed or delivered.

16 (4) For the purposes of this Part, a person does not provide an
17 electronic service merely because the person provides a billing
18 service, or a fee collection service, in relation to an electronic
19 service.

20 (5) A reference in this section to the *use* of a thing is a reference to the
21 use of the thing either:

22 (a) in isolation; or

23 (b) in conjunction with one or more other things.

24 **317E Listed acts or things**

25 (1) For the purposes of the application of this Part to a designated
26 communications provider, *listed act or thing* means:

27 (a) removing one or more forms of electronic protection that are
28 or were applied by, or on behalf of, the provider; or

29 (b) providing technical information; or

30 (c) installing, maintaining, testing or using software or
31 equipment; or

- 1 (d) ensuring that information obtained in connection with the
2 execution of a warrant or authorisation is given in a particular
3 format; or
4 (da) an act or thing done to assist in, or facilitate:
5 (i) giving effect to a warrant or authorisation under a law of
6 the Commonwealth, a State or a Territory; or
7 (ii) the effective receipt of information in connection with a
8 warrant or authorisation under a law of the
9 Commonwealth, a State or a Territory; or
10 (e) facilitating or assisting access to whichever of the following
11 are the subject of eligible activities of the provider:
12 (i) a facility;
13 (ii) customer equipment;
14 (iii) a data processing device;
15 (iv) a listed carriage service;
16 (v) a service that facilitates, or is ancillary or incidental to,
17 the supply of a listed carriage service;
18 (vi) an electronic service;
19 (vii) a service that facilitates, or is ancillary or incidental to,
20 the provision of an electronic service;
21 (viii) software used, for use, or likely to be used, in
22 connection with a listed carriage service;
23 (ix) software used, for use, or likely to be used, in
24 connection with an electronic service;
25 (x) software that is capable of being installed on a
26 computer, or other equipment, that is, or is likely to be,
27 connected to a telecommunications network; or
28 (f) assisting with the testing, modification, development or
29 maintenance of a technology or capability; or
30 (g) notifying particular kinds of changes to, or developments
31 affecting, eligible activities of the designated
32 communications provider, if the changes are relevant to the
33 execution of a warrant or authorisation; or
34 (h) modifying, or facilitating the modification of, any of the
35 characteristics of a service provided by the designated
36 communications provider; or
37 (i) substituting, or facilitating the substitution of, a service
38 provided by the designated communications provider for:
-

- 1 (i) another service provided by the provider; or
2 (ii) a service provided by another designated
3 communications provider; or
4 (j) an act or thing done to conceal the fact that any thing has
5 been done covertly in the performance of a function, or the
6 exercise of a power, conferred by a law of the
7 Commonwealth, a State or a Territory, so far as the function
8 or power relates to:
9 (i) enforcing the criminal law, so far as it relates to serious
10 Australian offences; or
11 (ii) assisting the enforcement of the criminal laws in force
12 in a foreign country, so far as those laws relate to
13 serious foreign offences; or
14 (iii) the interests of Australia's national security, the
15 interests of Australia's foreign relations or the interests
16 of Australia's national economic well-being.
- 17 (2) Paragraph (1)(j) does not apply to:
18 (a) making a false or misleading statement; or
19 (b) engaging in dishonest conduct.

317F Extension to external Territories

20 This Part extends to every external Territory.

Division 2—Voluntary technical assistance

317G Voluntary technical assistance provided to ASIO, the Australian Secret Intelligence Service, the Australian Signals Directorate or an interception agency

- 26 (1) If:
27 (a) any of the following persons:
28 (i) the Director-General of Security;
29 (ii) the Director-General of the Australian Secret
30 Intelligence Service;
31 (iii) the Director-General of the Australian Signals
32 Directorate;
33 (iv) the chief officer of an interception agency;
-

- 1 requests a designated communications provider to do one or
2 more specified acts or things that:
- 3 (v) are in connection with any or all of the eligible activities
4 of the provider; and
 - 5 (vi) are covered by subsection (2); and
- 6 (b) the provider does an act or thing:
- 7 (i) in accordance with the request; or
 - 8 (ii) in good faith purportedly in accordance with the
9 request;
- 10 then:
- 11 (c) the provider is not subject to any civil liability for, or in
12 relation to, the act or thing mentioned in paragraph (b); and
 - 13 (d) an officer, employee or agent of the provider is not subject to
14 any civil liability for, or in relation to, an act or thing done by
15 the officer, employee or agent in connection with the act or
16 thing mentioned in paragraph (b).
- 17 (2) The specified acts or things must:
- 18 (a) be directed towards ensuring that the designated
19 communications provider is capable of giving help to:
 - 20 (i) in a case where the request is made by the
21 Director-General of Security—ASIO; or
 - 22 (ii) in a case where the request is made by the
23 Director-General of the Australian Secret Intelligence
24 Service—the Australian Secret Intelligence Service; or
 - 25 (iii) in a case where the request is made by the
26 Director-General of the Australian Signals
27 Directorate—the Australian Signals Directorate; or
 - 28 (iv) in a case where the request is made by the chief officer
29 of an interception agency—the agency;
 - 30 in relation to:
 - 31 (v) the performance of a function, or the exercise of a
32 power, conferred by or under a law of the
33 Commonwealth, a State or a Territory, so far as the
34 function or power relates to a relevant objective; or
 - 35 (vi) a matter that facilitates, or is ancillary or incidental to, a
36 matter covered by subparagraph (v); or
 - 37 (b) be by way of giving help to:
-

- 1 (i) in a case where the request is made by the
2 Director-General of Security—ASIO; or
3 (ii) in a case where the request is made by the
4 Director-General of the Australian Secret Intelligence
5 Service—the Australian Secret Intelligence Service; or
6 (iii) in a case where the request is made by the
7 Director-General of the Australian Signals
8 Directorate—the Australian Signals Directorate; or
9 (iv) in a case where the request is made by the chief officer
10 of an interception agency—the agency;
11 in relation to:
12 (v) the performance of a function, or the exercise of a
13 power, conferred by or under a law of the
14 Commonwealth, a State or a Territory, so far as the
15 function or power relates to a relevant objective; or
16 (vi) a matter that facilitates, or is ancillary or incidental to, a
17 matter covered by subparagraph (v).
- 18 (3) A request under paragraph (1)(a) is to be known as a *technical*
19 *assistance request*.
- 20 (4) Subparagraph (1)(b)(ii) does not apply to an act or thing done by a
21 designated communications provider unless the act or thing is in
22 connection with any or all of the eligible activities of the provider.
- 23 *Relevant objective*
- 24 (5) For the purposes of this section, *relevant objective* means:
25 (a) in relation to a technical assistance request given by the
26 Director-General of Security—safeguarding national
27 security; or
28 (b) in relation to a technical assistance request given by the
29 Director-General of the Australian Secret Intelligence
30 Service—the interests of Australia’s national security, the
31 interests of Australia’s foreign relations or the interests of
32 Australia’s national economic well-being; or
33 (c) in relation to a technical assistance request given by the
34 Director-General of the Australian Signals Directorate—
35 providing material, advice and other assistance to a person or
36 body mentioned in subsection 7(2) of the *Intelligence*
-

- 1 *Services Act 2001* on matters relating to the security and
2 integrity of information that is processed, stored or
3 communicated by electronic or similar means; or
4 (d) in relation to a technical assistance request given by the chief
5 officer of an interception agency:
6 (i) enforcing the criminal law, so far as it relates to serious
7 Australian offences; or
8 (ii) assisting the enforcement of the criminal laws in force
9 in a foreign country, so far as those laws relate to
10 serious foreign offences.

11 *Listed acts or things*

- 12 (6) The acts or things that may be specified in a technical assistance
13 request given to a designated communications provider include
14 (but are not limited to) listed acts or things, so long as those acts or
15 things:
16 (a) are in connection with any or all of the eligible activities of
17 the provider; and
18 (b) are covered by subsection (2).

19 Note: For *listed acts or things*, see section 317E.

20 **317H Form of technical assistance request**

- 21 (1) A technical assistance request may be given:
22 (a) orally; or
23 (b) in writing.
24 (2) A technical assistance request must not be given orally unless:
25 (a) an imminent risk of serious harm to a person or substantial
26 damage to property exists; and
27 (b) the technical assistance request is necessary for the purpose
28 of dealing with that risk; and
29 (c) it is not practicable in the circumstances to give the technical
30 assistance request in writing.
31 (3) If a technical assistance request is given orally by:
32 (a) the Director-General of Security; or

- 1 (b) the Director-General of the Australian Secret Intelligence
2 Service; or
3 (c) the Director-General of the Australian Signals Directorate; or
4 (d) the chief officer of an interception agency;
5 the Director-General of Security, the Director-General of the
6 Australian Secret Intelligence Service, the Director-General of the
7 Australian Signals Directorate or the chief officer, as the case
8 requires, must:
9 (e) make a written record of the request; and
10 (f) do so within 48 hours after the request was given.
- 11 (4) If, under subsection (3):
12 (a) the Director-General of Security; or
13 (b) the Director-General of the Australian Secret Intelligence
14 Service; or
15 (c) the Director-General of the Australian Signals Directorate; or
16 (d) the chief officer of an interception agency;
17 makes a written record of a technical assistance request, the
18 Director-General of Security, the Director-General of the
19 Australian Secret Intelligence Service, the Director-General of the
20 Australian Signals Directorate or the chief officer, as the case
21 requires, must:
22 (e) give a copy of the record to the designated communications
23 provider concerned; and
24 (f) do so as soon as practicable after the record was made.
- 25 (5) If, under subsection (3):
26 (a) the Director-General of Security; or
27 (b) the Director-General of the Australian Secret Intelligence
28 Service; or
29 (c) the Director-General of the Australian Signals Directorate; or
30 (d) the chief officer of an interception agency;
31 makes a written record of a technical assistance request, the
32 Director-General of Security, the Director-General of the
33 Australian Secret Intelligence Service, the Director-General of the
34 Australian Signals Directorate or the chief officer, as the case
35 requires, must retain the record while the request is in force.

1 **317HAA Provision of advice to designated communications**
2 **providers**

- 3 (1) If the Director-General of Security gives a technical assistance
4 request to a designated communications provider, the
5 Director-General of Security must advise the provider that
6 compliance with the request is voluntary.
- 7 (2) If the Director-General of the Australian Secret Intelligence
8 Service gives a technical assistance request to a designated
9 communications provider, the Director-General of the Australian
10 Secret Intelligence Service must advise the provider that
11 compliance with the request is voluntary.
- 12 (3) If the Director-General of the Australian Signals Directorate gives
13 a technical assistance request to a designated communications
14 provider, the Director-General of the Australian Signals
15 Directorate must advise the provider that compliance with the
16 request is voluntary.
- 17 (4) If the chief officer of an interception agency gives a technical
18 assistance request to a designated communications provider, the
19 chief officer must advise the provider that compliance with the
20 request is voluntary.

21 *Form of advice*

- 22 (5) Advice under subsection (1), (2), (3) or (4) may be given:
23 (a) orally; or
24 (b) in writing.
- 25 (6) If advice under subsection (1), (2), (3) or (4) is given orally by:
26 (a) the Director-General of Security; or
27 (b) the Director-General of the Australian Secret Intelligence
28 Service; or
29 (c) the Director-General of the Australian Signals Directorate; or
30 (d) the chief officer of an interception agency;
31 the Director-General of Security, the Director-General of the
32 Australian Secret Intelligence Service, the Director-General of the
33 Australian Signals Directorate or the chief officer, as the case
34 requires, must:

- 1 (e) make a written record of the advice; and
2 (f) do so within 48 hours after the advice was given.

3 **317HAB Notification obligations**

- 4 (1) If the Director-General of Security gives a technical assistance
5 request, the Director-General of Security must, within 7 days after
6 the request is given, notify the Inspector-General of Intelligence
7 and Security that the request has been given.
- 8 (2) If the Director-General of the Australian Secret Intelligence
9 Service gives a technical assistance request, the Director-General
10 of the Australian Secret Intelligence Service must, within 7 days
11 after the request is given, notify the Inspector-General of
12 Intelligence and Security that the request has been given.
- 13 (3) If the Director-General of the Australian Signals Directorate gives
14 a technical assistance request, the Director-General of the
15 Australian Signals Directorate must, within 7 days after the request
16 is given, notify the Inspector-General of Intelligence and Security
17 that the request has been given.
- 18 (4) If the chief officer of an interception agency gives a technical
19 assistance request, the chief officer must, within 7 days after the
20 request is given, notify the Commonwealth Ombudsman that the
21 request has been given.
- 22 (5) A failure to comply with subsection (1), (2), (3) or (4) does not
23 affect the validity of a technical assistance request.

24 **317HA Duration of technical assistance request**

- 25 (1) A technical assistance request:
26 (a) comes in force:
27 (i) when it is given; or
28 (ii) if a later time is specified in the request—at that later
29 time; and
30 (b) unless sooner revoked, remains in force:
31 (i) if an expiry date is specified in the request—until the
32 start of the expiry date; or

1 (ii) otherwise—at end of the 90-day period beginning when
2 the request was given.

3 (2) If a technical assistance request expires, this Part does not prevent
4 the giving of a fresh technical assistance request in the same terms
5 as the expired technical assistance request.

6 **317J Specified period etc.**

7 (1) A technical assistance request may include a request that a
8 specified act or thing be done within a specified period.

9 (2) A technical assistance request may include a request that a
10 specified act or thing be done:
11 (a) in a specified manner; or
12 (b) in a way that meets one or more specified conditions.

13 (3) Subsections (1) and (2) of this section do not limit
14 subsections 317G(1) and (2).

15 **317JAA Decision-making criteria**

16 (1) The Director-General of Security must not give a technical
17 assistance request to a designated communications provider unless
18 the Director-General of Security is satisfied that:
19 (a) the request is reasonable and proportionate; and
20 (b) compliance with the request is:
21 (i) practicable; and
22 (ii) technically feasible.

23 Note: See also section 317JC.

24 (2) The Director-General of the Australian Secret Intelligence Service
25 must not give a technical assistance request to a designated
26 communications provider unless the Director-General of the
27 Australian Secret Intelligence Service is satisfied that:
28 (a) the request is reasonable and proportionate; and
29 (b) compliance with the request is:
30 (i) practicable; and
31 (ii) technically feasible.

32 Note: See also section 317JC.

- 1 (3) The Director-General of the Australian Signals Directorate must
2 not give a technical assistance request to a designated
3 communications provider unless the Director-General of the
4 Australian Signals Directorate is satisfied that:
5 (a) the request is reasonable and proportionate; and
6 (b) compliance with the request is:
7 (i) practicable; and
8 (ii) technically feasible.

9 Note: See also section 317JC.

- 10 (4) The chief officer of an interception agency must not give a
11 technical assistance request to a designated communications
12 provider unless the chief officer is satisfied that:
13 (a) the request is reasonable and proportionate; and
14 (b) compliance with the request is:
15 (i) practicable; and
16 (ii) technically feasible.

17 Note: See also section 317JC.

18 **317JA Variation of technical assistance requests**

- 19 (1) If a technical assistance request has been given to a designated
20 communications provider by the Director-General of Security, the
21 Director-General of Security may vary the request.
- 22 (2) If a technical assistance request has been given to a designated
23 communications provider by the Director-General of the Australian
24 Secret Intelligence Service, the Director-General of the Australian
25 Secret Intelligence Service may vary the request.
- 26 (3) If a technical assistance request has been given to a designated
27 communications provider by the Director-General of the Australian
28 Signals Directorate, the Director-General of the Australian Signals
29 Directorate may vary the request.
- 30 (4) If a technical assistance request has been given to a designated
31 communications provider by the chief officer of an interception
32 agency, the chief officer may vary the request.

1 *Form of variation*

2 (5) A variation may be made:

- 3 (a) orally; or
4 (b) in writing.

5 (6) A variation must not be made orally unless:

- 6 (a) an imminent risk of serious harm to a person or substantial
7 damage to property exists; and
8 (b) the variation is necessary for the purpose of dealing with that
9 risk; and
10 (c) it is not practicable in the circumstances to make the
11 variation in writing.

12 (7) If a variation is made orally by:

- 13 (a) the Director-General of Security; or
14 (b) the Director-General of the Australian Secret Intelligence
15 Service; or
16 (c) the Director-General of the Australian Signals Directorate; or
17 (d) the chief officer of an interception agency;

18 the Director-General of Security, the Director-General of the
19 Australian Secret Intelligence Service, the Director-General of the
20 Australian Signals Directorate or the chief officer, as the case
21 requires, must:

- 22 (e) make a written record of the variation; and
23 (f) do so within 48 hours after the variation was made.

24 (8) If, under subsection (7):

- 25 (a) the Director-General of Security; or
26 (b) the Director-General of the Australian Secret Intelligence
27 Service; or
28 (c) the Director-General of the Australian Signals Directorate; or
29 (d) the chief officer of an interception agency;

30 makes a written record of a variation, the Director-General of
31 Security, the Director-General of the Australian Secret Intelligence
32 Service, the Director-General of the Australian Signals Directorate
33 or the chief officer, as the case requires, must:

- 34 (e) give a copy of the record to the designated communications
35 provider concerned; and
-

1 (f) do so as soon as practicable after the record was made.

2 *Acts or things specified in a varied technical assistance request*

3 (9) The acts or things specified in a varied technical assistance request
4 must be:

5 (a) in connection with any or all of the eligible activities of the
6 designated communications provider concerned; and

7 (b) covered by subsection 317G(2).

8 (10) The acts or things that may be specified in a varied technical
9 assistance request include (but are not limited to) listed acts or
10 things, so long as those acts or things:

11 (a) are in connection with any or all of the eligible activities of
12 the designated communications provider concerned; and

13 (b) are covered by subsection 317G(2).

14 Note: For *listed acts or things*, see section 317E.

15 *Decision-making criteria*

16 (11) The Director-General of Security must not vary a technical
17 assistance request unless the Director-General of Security is
18 satisfied that:

19 (a) the varied request is reasonable and proportionate; and

20 (b) compliance with the varied request is:

21 (i) practicable; and

22 (ii) technically feasible.

23 Note: See also section 317JC.

24 (12) The Director-General of the Australian Secret Intelligence Service
25 must not vary a technical assistance request unless the
26 Director-General of the Australian Secret Intelligence Service is
27 satisfied that:

28 (a) the varied request is reasonable and proportionate; and

29 (b) compliance with the varied request is:

30 (i) practicable; and

31 (ii) technically feasible.

32 Note: See also section 317JC.

- 1 (13) The Director-General of the Australian Signals Directorate must
2 not vary a technical assistance request unless the Director-General
3 of the Australian Signals Directorate is satisfied that:
4 (a) the varied request is reasonable and proportionate; and
5 (b) compliance with the varied request is:
6 (i) practicable; and
7 (ii) technically feasible.

8 Note: See also section 317JC.

- 9 (14) The chief officer of an interception agency must not vary a
10 technical assistance request unless the chief officer is satisfied that:
11 (a) the varied request is reasonable and proportionate; and
12 (b) compliance with the varied request is:
13 (i) practicable; and
14 (ii) technically feasible.

15 Note: See also section 317JC.

16 *Notification obligations*

- 17 (15) If the Director-General of Security varies a technical assistance
18 request, the Director-General of Security must, within 7 days after
19 varying the request, notify the Inspector-General of Intelligence
20 and Security that the request has been varied.
- 21 (16) If the Director-General of the Australian Secret Intelligence
22 Service varies a technical assistance request, the Director-General
23 of the Australian Secret Intelligence Service must, within 7 days
24 after varying the request, notify the Inspector-General of
25 Intelligence and Security that the request has been varied.
- 26 (17) If the Director-General of the Australian Signals Directorate varies
27 a technical assistance request, the Director-General of the
28 Australian Signals Directorate must, within 7 days after varying the
29 request, notify the Inspector-General of Intelligence and Security
30 that the request has been varied.
- 31 (18) If the chief officer of an interception agency varies a technical
32 assistance request, the chief officer must, within 7 days after
33 varying the request, notify the Commonwealth Ombudsman that
34 the request has been varied.

- 1 (19) A failure to comply with subsection (15), (16), (17) or (18) does
2 not affect the validity of a variation of a technical assistance
3 request.

4 **317JB Revocation of technical assistance requests**

- 5 (1) If a technical assistance request has been given to a person by the
6 Director-General of Security, the Director-General of Security
7 may, by written notice given to the person, revoke the request.
- 8 (1A) If a technical assistance request has been given to a person by the
9 Director-General of Security, and the Director-General of Security
10 is satisfied that:
11 (a) the request is not reasonable and proportionate; or
12 (b) compliance with the request is not:
13 (i) practicable; and
14 (ii) technically feasible;
15 the Director-General of Security must, by written notice given to
16 the person, revoke the request.
- 17 (2) If a technical assistance request has been given to a person by the
18 Director-General of the Australian Secret Intelligence Service, the
19 Director-General of the Australian Secret Intelligence Service may,
20 by written notice given to the person, revoke the request.
- 21 (2A) If a technical assistance request has been given to a person by the
22 Director-General of the Australian Secret Intelligence Service, and
23 the Director-General of the Australian Secret Intelligence Service
24 is satisfied that:
25 (a) the request is not reasonable and proportionate; or
26 (b) compliance with the request is not:
27 (i) practicable; and
28 (ii) technically feasible;
29 the Director-General of the Australian Secret Intelligence Service
30 must, by written notice given to the person, revoke the request.
- 31 (3) If a technical assistance request has been given to a person by the
32 Director-General of the Australian Signals Directorate, the
33 Director-General of the Australian Signals Directorate may, by
34 written notice given to the person, revoke the request.

- 1 (3A) If a technical assistance request has been given to a person by the
2 Director-General of the Australian Signals Directorate, and the
3 Director-General of the Australian Signals Directorate is satisfied
4 that:
5 (a) the request is not reasonable and proportionate; or
6 (b) compliance with the request is not:
7 (i) practicable; and
8 (ii) technically feasible;
9 the Director-General of the Australian Signals Directorate must, by
10 written notice given to the person, revoke the request.
- 11 (4) If a technical assistance request has been given to a person by the
12 chief officer of an interception agency, the chief officer may, by
13 written notice given to the person, revoke the request.
- 14 (5) If a technical assistance request has been given to a person by the
15 chief officer of an interception agency, and the chief officer is
16 satisfied that:
17 (a) the request is not reasonable and proportionate; or
18 (b) compliance with the request is not:
19 (i) practicable; and
20 (ii) technically feasible;
21 the chief officer must, by written notice given to the person, revoke
22 the request.
- 23 *Notification obligations*
- 24 (6) If the Director-General of Security revokes a technical assistance
25 request, the Director-General of Security must, within 7 days after
26 revoking the request, notify the Inspector-General of Intelligence
27 and Security that the request has been revoked.
- 28 (7) If the Director-General of the Australian Secret Intelligence
29 Service revokes a technical assistance request, the
30 Director-General of the Australian Secret Intelligence Service
31 must, within 7 days after revoking the request, notify the
32 Inspector-General of Intelligence and Security that the request has
33 been revoked.

- 1 (8) If the Director-General of the Australian Signals Directorate
2 revokes a technical assistance request, the Director-General of the
3 Australian Signals Directorate must, within 7 days after revoking
4 the request, notify the Inspector-General of Intelligence and
5 Security that the request has been revoked.
- 6 (9) If the chief officer of an interception agency revokes a technical
7 assistance request, the chief officer must, within 7 days after
8 revoking the request, notify the Commonwealth Ombudsman that
9 the request has been revoked.
- 10 (10) A failure to comply with subsection (6), (7), (8) or (9) does not
11 affect the validity of a revocation of a technical assistance request.

12 **317JC Whether a technical assistance request is reasonable and**
13 **proportionate**

14 In considering whether a technical assistance request or a varied
15 technical assistance request is reasonable and proportionate, the
16 Director-General of Security, the Director-General of the
17 Australian Secret Intelligence Service, the Director-General of the
18 Australian Signals Directorate or the chief officer of an
19 interception agency, as the case requires, must have regard to the
20 following matters:

- 21 (a) the interests of national security;
22 (b) the interests of law enforcement;
23 (c) the legitimate interests of the designated communications
24 provider to whom the request relates;
25 (d) the objectives of the request;
26 (e) the availability of other means to achieve the objectives of
27 the request;
28 (f) whether the request, when compared to other forms of
29 industry assistance known to the Director-General of
30 Security, the Director-General of the Australian Secret
31 Intelligence Service, the Director-General of the Australian
32 Signals Directorate or the chief officer, as the case requires,
33 is the least intrusive form of industry assistance so far as the
34 following persons are concerned:
35 (i) persons whose activities are not of interest to ASIO;

- 1 (ii) persons whose activities are not of interest to the
2 Australian Secret Intelligence Service;
3 (iii) persons whose activities are not of interest to the
4 Australian Signals Directorate;
5 (iv) persons whose activities are not of interest to
6 interception agencies;
7 (g) whether the request is necessary;
8 (h) the legitimate expectations of the Australian community
9 relating to privacy and cybersecurity;
10 (i) such other matters (if any) as the Director-General of
11 Security, the Director-General of the Australian Secret
12 Intelligence Service, the Director-General of the Australian
13 Signals Directorate or the chief officer, as the case requires,
14 considers relevant.

15 **317K Contract etc.**

- 16 Any of the following persons:
17 (a) the Director-General of Security;
18 (b) the Director-General of the Australian Secret Intelligence
19 Service;
20 (c) the Director-General of the Australian Signals Directorate;
21 (d) the chief officer of an interception agency;
22 may enter into a contract, agreement or arrangement with a
23 designated communications provider in relation to acts or things
24 done by the provider in accordance with a technical assistance
25 request.

26 **Division 3—Technical assistance notices**

27 **317L Technical assistance notices**

- 28 (1) The Director-General of Security or the chief officer of an
29 interception agency may give a designated communications
30 provider a notice, to be known as a technical assistance notice, that
31 requires the provider to do one or more specified acts or things
32 that:
33 (a) are in connection with any or all of the eligible activities of
34 the provider; and
-

Schedule 1 Industry assistance
Part 1 Amendments

1 (b) are covered by subsection (2).

2 Note: Section 317ZK deals with the terms and conditions on which such a
3 requirement is to be complied with.

4 (2) The specified acts or things must be by way of giving help to:

5 (a) in a case where the technical assistance notice is given by the
6 Director-General of Security—ASIO; or

7 (b) in a case where the technical assistance notice is given by the
8 chief officer of an interception agency—the agency;

9 in relation to:

10 (c) the performance of a function, or the exercise of a power,
11 conferred by or under a law of the Commonwealth, a State or
12 a Territory, so far as the function or power relates to:

13 (i) enforcing the criminal law, so far as it relates to serious
14 Australian offences; or

15 (ii) assisting the enforcement of the criminal laws in force
16 in a foreign country, so far as those laws relate to
17 serious foreign offences; or

18 (iii) safeguarding national security; or

19 (d) a matter that facilitates, or is ancillary or incidental to, a
20 matter covered by paragraph (c).

21 (2A) The specified acts or things must not be directed towards ensuring
22 that a designated communications provider is capable of giving
23 help to ASIO or an interception agency.

24 *Listed acts or things*

25 (3) The acts or things specified in a technical assistance notice given to
26 a designated communications provider must be listed acts or
27 things, so long as those acts or things:

28 (a) are in connection with any or all of the eligible activities of
29 the provider; and

30 (b) are covered by subsection (2).

31 Note: For *listed acts or things*, see section 317E.

1 **317LA Approval of technical assistance notices given by the chief**
2 **officer of an interception agency of a State or Territory**

- 3 (1) The chief officer of an interception agency of a State or Territory
4 must not give a technical assistance notice to a designated
5 communications provider unless:
6 (a) the chief officer has given the AFP Commissioner a written
7 notice setting out a proposal to give the technical assistance
8 notice; and
9 (b) the AFP Commissioner has approved the giving of the
10 technical assistance notice.
- 11 (2) An approval under paragraph (1)(b) may be given:
12 (a) orally; or
13 (b) in writing.
- 14 (3) If an approval under paragraph (1)(b) is given orally, the AFP
15 Commissioner must:
16 (a) make a written record of the approval; and
17 (b) do so within 48 hours after the approval was given.
- 18 (4) For the purposes of this section, **AFP Commissioner** means the
19 Commissioner (within the meaning of the *Australian Federal*
20 *Police Act 1979*).

21 **317M Form of technical assistance notice**

- 22 (1) A technical assistance notice may be given:
23 (a) orally; or
24 (b) in writing.
- 25 (2) A technical assistance notice must not be given orally unless:
26 (a) an imminent risk of serious harm to a person or substantial
27 damage to property exists; and
28 (b) the technical assistance notice is necessary for the purpose of
29 dealing with that risk; and
30 (c) it is not practicable in the circumstances to give the technical
31 assistance notice in writing.

- 1 (3) If a technical assistance notice is given orally by the
2 Director-General of Security or the chief officer of an interception
3 agency, the Director-General of Security or the chief officer, as the
4 case requires, must:
5 (a) make a written record of the notice; and
6 (b) do so within 48 hours after the notice was given.
- 7 (4) If, under subsection (3), the Director-General of Security or the
8 chief officer of an interception agency makes a written record of a
9 technical assistance notice, the Director-General of Security or the
10 chief officer, as the case requires, must:
11 (a) give a copy of the record to the designated communications
12 provider concerned; and
13 (b) do so as soon as practicable after the record was made.
- 14 (5) If, under subsection (3), the Director-General of Security or the
15 chief officer of an interception agency makes a written record of a
16 technical assistance notice, the Director-General of Security or the
17 chief officer, as the case requires, must retain the record while the
18 notice is in force.

19 **317MAA Provision of advice to designated communications**
20 **providers**

- 21 (1) If the Director-General of Security gives a technical assistance
22 notice to a designated communications provider, the
23 Director-General of Security must give the provider advice relating
24 to the provider's obligations under whichever of sections 317ZA
25 and 317ZB is applicable, so far as those obligations relate to the
26 notice.
- 27 (2) If the chief officer of an interception agency gives a technical
28 assistance notice to a designated communications provider, the
29 chief officer must give the provider advice relating to the
30 provider's obligations under whichever of sections 317ZA and
31 317ZB is applicable, so far as those obligations relate to the notice.
- 32 (3) If the Director-General of Security gives a technical assistance
33 notice to a designated communications provider, the
34 Director-General of Security must notify the provider of the
35 provider's right to make a complaint about the notice to the

1 Inspector-General of Intelligence and Security under the
2 *Inspector-General of Intelligence and Security Act 1986*.

3 (4) If:

4 (a) the chief officer of an interception agency gives a technical
5 assistance notice to a designated communications provider;
6 and

7 (b) the provider has a right to make a complaint about the
8 conduct of the chief officer, or the interception agency, in
9 relation to the notice to:

10 (i) the Commonwealth Ombudsman; or

11 (ii) an authority that is the State or Territory inspecting
12 agency in relation to the interception agency;

13 the chief officer must notify the provider of the provider's right to
14 make such a complaint.

15 *Form of advice or notification*

16 (5) Advice under subsection (1) or (2), or notification under
17 subsection (3) or (4), may be given:

18 (a) orally; or

19 (b) in writing.

20 (6) If advice under subsection (1) or (2), or notification under
21 subsection (3) or (4), is given orally by the Director-General of
22 Security or the chief officer of an interception agency, the
23 Director-General of Security or the chief officer, as the case
24 requires, must:

25 (a) make a written record of the advice or notification; and

26 (b) do so within 48 hours after the advice or notification was
27 given.

28 **317MAB Notification obligations**

29 (1) If the Director-General of Security gives a technical assistance
30 notice, the Director-General of Security must, within 7 days after
31 the notice is given, notify the Inspector-General of Intelligence and
32 Security that the notice has been given.

- 1 (2) If the chief officer of an interception agency gives a technical
2 assistance notice, the chief officer must, within 7 days after the
3 notice is given, notify the Commonwealth Ombudsman that the
4 notice has been given.
- 5 (3) A failure to comply with subsection (1) or (2) does not affect the
6 validity of a technical assistance notice.

7 **317MA Duration of technical assistance notice**

- 8 (1) A technical assistance notice:
9 (a) comes in force:
10 (i) when it is given; or
11 (ii) if a later time is specified in the notice—at that later
12 time; and
13 (b) unless sooner revoked, remains in force:
14 (i) if an expiry date is specified in the notice—until the
15 start of the expiry date; or
16 (ii) otherwise—at end of the 90-day period beginning when
17 the notice was given.
- 18 (1A) An expiry date specified in a technical assistance notice must not
19 be later than 12 months after the notice was given.
- 20 (1B) Paragraph (1)(b) has effect subject to subsections (1C) and (1D).
- 21 (1C) If the Director-General of Security has given a technical assistance
22 notice to a designated communications provider, the
23 Director-General of Security may, with the agreement of the
24 provider, extend for a further period (not exceeding 12 months) or
25 further periods (not exceeding 12 months in each case) the period
26 for which the technical assistance notice is in force.
- 27 (1D) If the chief officer of an interception agency has given a technical
28 assistance notice to a designated communications provider, the
29 chief officer may, with the agreement of the provider, extend for a
30 further period (not exceeding 12 months) or further periods (not
31 exceeding 12 months in each case) the period for which the
32 technical assistance notice is in force.

- 1 (1E) If the Director-General of Security extends the period for which a
2 technical assistance notice is in force, the Director-General of
3 Security must, within 7 days after extending the period, notify the
4 Inspector-General of Intelligence and Security of the extension.
- 5 (1F) If the chief officer of an interception agency extends the period for
6 which a technical assistance notice is in force, the chief officer
7 must, within 7 days after extending the period, notify the
8 Commonwealth Ombudsman of the extension.
- 9 (1G) A failure to comply with subsection (1E) or (1F) does not affect the
10 validity of an extension of a technical assistance notice.
- 11 (2) If a technical assistance notice expires, this Part does not prevent
12 the giving of a fresh technical assistance notice in the same terms
13 as the expired technical assistance notice.

14 **317N Compliance period etc.**

- 15 (1) A technical assistance notice may require a specified act or thing to
16 be done within a specified period.
- 17 (2) A technical assistance notice may require a specified act or thing to
18 be done:
19 (a) in a specified manner; or
20 (b) in a way that meets one or more specified conditions.
- 21 (3) Subsections (1) and (2) of this section do not limit
22 subsections 317L(1) and (2).

23 **317P Decision-making criteria**

- 24 The Director-General of Security or the chief officer of an
25 interception agency must not give a technical assistance notice to a
26 designated communications provider unless the Director-General
27 of Security or the chief officer, as the case requires, is satisfied
28 that:
29 (a) the requirements imposed by the notice are reasonable and
30 proportionate; and
31 (b) compliance with the notice is:
32 (i) practicable; and

1 (ii) technically feasible.

2 Note: See also section 317RA.

3 **317PA Consultation about a proposal to give a technical assistance**
4 **notice**

5 (1) Before giving a technical assistance notice to a designated
6 communications provider, the Director-General of Security or the
7 chief officer of an interception agency, as the case requires, must
8 consult the provider.

9 (2) The rule in subsection (1) does not apply to a technical assistance
10 notice given to a designated communications provider by the
11 Director-General of Security if:

12 (a) the Director-General of Security is satisfied that the technical
13 assistance notice should be given as a matter of urgency; or

14 (b) the provider waives compliance with subsection (1).

15 (3) The rule in subsection (1) does not apply to a technical assistance
16 notice given to a designated communications provider by the chief
17 officer of an interception agency if:

18 (a) the chief officer is satisfied that the technical assistance
19 notice should be given as a matter of urgency; or

20 (b) the provider waives compliance with subsection (1).

21 **317Q Variation of technical assistance notices**

22 (1) If a technical assistance notice has been given to a designated
23 communications provider by the Director-General of Security, the
24 Director-General of Security may vary the notice.

25 (2) If a technical assistance notice has been given to a designated
26 communications provider by the chief officer of an interception
27 agency, the chief officer may vary the notice.

28 *Form of variation*

29 (3) A variation may be made:

30 (a) orally; or

31 (b) in writing.

- 1 (4) A variation must not be made orally unless:
2 (a) an imminent risk of serious harm to a person or substantial
3 damage to property exists; and
4 (b) the variation is necessary for the purpose of dealing with that
5 risk; and
6 (c) it is not practicable in the circumstances to make the
7 variation in writing.
- 8 (5) If a variation is made orally by the Director-General of Security or
9 the chief officer of an interception agency, the Director-General of
10 Security or the chief officer, as the case requires, must:
11 (a) make a written record of the variation; and
12 (b) do so within 48 hours after the variation was made.
- 13 (6) If, under subsection (5), the Director-General of Security or the
14 chief officer of an interception agency makes a written record of a
15 variation, the Director-General of Security or the chief officer, as
16 the case requires, must:
17 (a) give a copy of the record to the designated communications
18 provider concerned; and
19 (b) do so as soon as practicable after the record was made.
- 20 (7) If a variation is made in writing by the Director-General of
21 Security or the chief officer of an interception agency, the
22 Director-General of Security or the chief officer, as the case
23 requires, must:
24 (a) give a copy of the variation to the designated
25 communications provider concerned; and
26 (b) do so as soon as practicable after the variation was made.
- 27 *Acts or things specified in a varied technical assistance notice*
- 28 (8) The acts or things specified in a varied technical assistance notice
29 must be:
30 (a) in connection with any or all of the eligible activities of the
31 designated communications provider concerned; and
32 (b) covered by subsection 317L(2).
- 33 (9) The acts or things specified in a varied technical assistance notice
34 must be listed acts or things, so long as those acts or things:
-

- 1 (a) are in connection with any or all of the eligible activities of
2 the designated communications provider concerned; and
3 (b) are covered by subsection 317L(2).

4 Note: For *listed acts or things*, see section 317E.

5 *Decision-making criteria*

- 6 (10) The Director-General of Security or the chief officer of an
7 interception agency must not vary a technical assistance notice
8 unless the Director-General of Security or the chief officer, as the
9 case requires, is satisfied that:
10 (a) the requirements imposed by the varied notice are reasonable
11 and proportionate; and
12 (b) compliance with the varied notice is:
13 (i) practicable; and
14 (ii) technically feasible.

15 Note: See also section 317RA.

16 *Variation must not extend duration of technical assistance notice*

- 17 (11) A variation of a technical assistance notice must not extend the
18 period for which the notice is in force.

19 *Notification obligations*

- 20 (12) If the Director-General of Security varies a technical assistance
21 notice, the Director-General of Security must, within 7 days after
22 varying the notice, notify the Inspector-General of Intelligence and
23 Security that the notice has been varied.
24 (13) If the chief officer of an interception agency varies a technical
25 assistance notice, the chief officer must, within 7 days after varying
26 the notice, notify the Commonwealth Ombudsman that the notice
27 has been varied.
28 (14) A failure to comply with subsection (12) or (13) does not affect the
29 validity of a variation of a technical assistance notice.

1 **317R Revocation of technical assistance notices**

- 2 (1) If a technical assistance notice has been given to a person by the
3 Director-General of Security, the Director-General of Security
4 may, by written notice given to the person, revoke the notice.
- 5 (2) If a technical assistance notice has been given to a person by the
6 Director-General of Security, and the Director-General of Security
7 is satisfied that:
8 (a) the requirements imposed by the notice are not reasonable
9 and proportionate; or
10 (b) compliance with the notice is not:
11 (i) practicable; and
12 (ii) technically feasible;
13 the Director-General of Security must, by written notice given to
14 the person, revoke the notice.
- 15 (3) If a technical assistance notice has been given to a person by the
16 chief officer of an interception agency, the chief officer may, by
17 written notice given to the person, revoke the notice.
- 18 (4) If a technical assistance notice has been given to a person by the
19 chief officer of an interception agency, and the chief officer is
20 satisfied that:
21 (a) the requirements imposed by the notice are not reasonable
22 and proportionate; or
23 (b) compliance with the notice is not:
24 (i) practicable; and
25 (ii) technically feasible;
26 the chief officer must, by written notice given to the person, revoke
27 the notice.
- 28 *Notification obligations*
- 29 (5) If the Director-General of Security revokes a technical assistance
30 notice, the Director-General of Security must, within 7 days after
31 revoking the notice, notify the Inspector-General of Intelligence
32 and Security that the notice has been revoked.
- 33 (6) If the chief officer of an interception agency revokes a technical
34 assistance notice, the chief officer must, within 7 days after

1 **Division 4—Technical capability notices**

2 **317S Attorney-General may determine procedures and**
3 **arrangements relating to requests for technical capability**
4 **notices**

- 5 (1) The Attorney-General may, by writing, determine procedures and
6 arrangements to be followed in relation to the making of requests
7 for technical capability notices.
- 8 (2) A procedure or arrangement determined under subsection (1) may
9 require that the agreement of a person or body must be obtained
10 before a request is made for a technical capability notice.
- 11 (3) A failure to comply with a determination under subsection (1) does
12 not affect the validity of a technical capability notice.
- 13 (4) A determination under subsection (1) is not a legislative
14 instrument.

15 **317T Technical capability notices**

- 16 (1) The Attorney-General may, in accordance with a request made by
17 the Director-General of Security or the chief officer of an
18 interception agency, give a designated communications provider a
19 written notice, to be known as a technical capability notice, that
20 requires the provider to do one or more specified acts or things
21 that:
22 (a) are in connection with any or all of the eligible activities of
23 the provider; and
24 (b) are covered by subsection (2).

25 Note: Section 317ZK deals with the terms and conditions on which such a
26 requirement is to be complied with.

- 27 (2) The specified acts or things must:
28 (a) be directed towards ensuring that the designated
29 communications provider is capable of giving listed help to
30 ASIO, or an interception agency, in relation to:
31 (i) the performance of a function, or the exercise of a
32 power, conferred by or under a law of the

- 1 Commonwealth, a State or a Territory, so far as the
2 function or power relates to a relevant objective; or
3 (ii) a matter that facilitates, or is ancillary or incidental to, a
4 matter covered by subparagraph (i); or
5 (b) be by way of giving help to ASIO, or an interception agency,
6 in relation to:
7 (i) the performance of a function, or the exercise of a
8 power, conferred by or under a law of the
9 Commonwealth, a State or a Territory, so far as the
10 function or power relates to a relevant objective; or
11 (ii) a matter that facilitates, or is ancillary or incidental to, a
12 matter covered by subparagraph (i).

13 *Relevant objective*

- 14 (3) For the purposes of this section, **relevant objective** means:
15 (a) enforcing the criminal law, so far as it relates to serious
16 Australian offences; or
17 (b) assisting the enforcement of the criminal laws in force in a
18 foreign country, so far as those laws relate to serious foreign
19 offences; or
20 (c) safeguarding national security.

21 *Listed help*

- 22 (4) For the purposes of the application of this section to a designated
23 communications provider, if one or more acts or things done by the
24 provider:
25 (a) are by way of giving help to ASIO or an interception agency;
26 and
27 (b) are in connection with any or all of the eligible activities of
28 the provider; and
29 (c) consist of either or both of the following:
30 (i) one or more listed acts or things (other than an act or
31 thing covered by paragraph 317E(1)(a));
32 (ii) one or more acts or things of a kind determined under
33 subsection (5);

34 that help is **listed help**.

35 Note: For **listed acts or things**, see section 317E.

- 1 (5) The Home Affairs Minister may, by legislative instrument,
2 determine one or more kinds of acts or things for the purposes of
3 subparagraph (4)(c)(ii).
- 4 (6) In making a determination under subsection (5), the Home Affairs
5 Minister must have regard to the following matters:
6 (a) the interests of law enforcement;
7 (b) the interests of national security;
8 (c) the objects of this Act;
9 (d) the likely impact of the determination on designated
10 communications providers;
11 (e) such other matters (if any) as the Home Affairs Minister
12 considers relevant.

13 *Listed acts or things*

- 14 (7) The acts or things specified in a technical capability notice given to
15 a designated communications provider in accordance with
16 paragraph (2)(b) must be listed acts or things, so long as those acts
17 or things:
18 (a) are in connection with any or all of the eligible activities of
19 the provider; and
20 (b) are covered by subsection (2), so far as that subsection relates
21 to paragraph (2)(b).

22 *Applicable costs negotiator*

- 23 (12) A technical capability notice must specify a person as the
24 applicable costs negotiator for the notice.

25 Note: See section 317ZK.

- 26 (13) A person may be specified under subsection (12):
27 (a) by name; or
28 (b) as any person from time to time holding, occupying, or
29 performing the duties of, a specified office or position.

30 **317TAAA Approval of technical capability notice**

- 31 (1) The Attorney-General must not give a technical capability notice to
32 a designated communications provider unless:
-

Schedule 1 Industry assistance
Part 1 Amendments

- 1 (a) the Attorney-General has given the Minister a written notice
2 setting out a proposal to give the technical capability notice;
3 and
4 (b) the Minister has approved the giving of the technical
5 capability notice.
- 6 (2) An approval under paragraph (1)(b) may be given:
7 (a) orally; or
8 (b) in writing.
- 9 (3) If an approval under paragraph (1)(b) is given orally, the Minister
10 must:
11 (a) make a written record of the approval; and
12 (b) do so within 48 hours after the approval was given.
- 13 (4) The Attorney-General may make a representation to the Minister
14 about the proposal to give the technical capability notice.
- 15 (5) A representation may deal with:
16 (a) any of the matters set out in section 317ZAA; and
17 (b) such other matters (if any) as the Attorney-General considers
18 relevant.
- 19 (6) In considering whether to approve the giving of the technical
20 capability notice, the Minister must have regard to the following
21 matters:
22 (a) the objectives of the notice;
23 (b) the legitimate interests of the designated communications
24 provider to whom the notice relates;
25 (c) the impact of the notice on the efficiency and international
26 competitiveness of the Australian telecommunications
27 industry;
28 (d) the representation (if any) that was made under
29 subsection (4);
30 (e) such other matters (if any) as the Minister considers relevant.

1 **317TAA Provision of advice to designated communications**
2 **providers**

- 3 (1) If the Attorney-General gives a technical capability notice to a
4 designated communications provider, the Attorney-General must
5 give the provider advice relating to the provider's obligations
6 under whichever of sections 317ZA and 317ZB is applicable, so
7 far as those obligations relate to the notice.

8 *Form of advice*

- 9 (2) Advice under subsection (1) may be given:
10 (a) orally; or
11 (b) in writing.
- 12 (3) If advice under subsection (1) is given orally, the Attorney-General
13 must:
14 (a) make a written record of the advice; and
15 (b) do so within 48 hours after the advice was given.

16 **317TAB Notification obligations**

- 17 (1) If:
18 (a) the Attorney-General gives a technical capability notice; and
19 (b) the acts or things specified in the notice:
20 (i) are directed towards ensuring that a designated
21 communications provider is capable of giving listed
22 help (within the meaning of section 317T) to ASIO in
23 relation to a matter covered by paragraph 317T(2)(a); or
24 (ii) are by way of giving help to ASIO in relation to a
25 matter covered by paragraph 317T(2)(b);
26 the Attorney-General must, within 7 days after the notice is given,
27 notify the Inspector-General of Intelligence and Security that the
28 notice has been given.

- 29 (2) If:
30 (a) the Attorney-General gives a technical capability notice; and
31 (b) the acts or things specified in the notice:
32 (i) are directed towards ensuring that a designated
33 communications provider is capable of giving listed

- 1 help (within the meaning of section 317T) to an
2 interception agency in relation to a matter covered by
3 paragraph 317T(2)(a); or
4 (ii) are by way of giving help to an interception agency in
5 relation to a matter covered by paragraph 317T(2)(b);
6 the Attorney-General must, within 7 days after the notice is given,
7 notify the Commonwealth Ombudsman that the notice has been
8 given.
- 9 (3) A failure to comply with subsection (1) or (2) does not affect the
10 validity of a technical capability notice.

11 **317TA Duration of technical capability notice**

- 12 (1) A technical capability notice:
13 (a) comes in force:
14 (i) when it is given; or
15 (ii) if a later time is specified in the notice—at that later
16 time; and
17 (b) unless sooner revoked, remains in force:
18 (i) if an expiry date is specified in the notice—until the
19 start of the expiry date; or
20 (ii) otherwise—at end of the 180-day period beginning
21 when the notice was given.
- 22 (1A) An expiry date specified in a technical capability notice must not
23 be later than 12 months after the notice was given.
- 24 (1B) Paragraph (1)(b) has effect subject to subsection (1C).
- 25 (1C) If the Attorney-General has given a technical capability notice to a
26 designated communications provider, the Attorney-General may,
27 with the agreement of the provider, extend for a further period (not
28 exceeding 12 months) or further periods (not exceeding 12 months
29 in each case) the period for which the technical capability notice is
30 in force.
- 31 (1D) If:
32 (a) the Attorney-General extends the period for which a
33 technical capability notice is in force; and

- 1 (b) the acts or things specified in the notice:
2 (i) are directed towards ensuring that a designated
3 communications provider is capable of giving listed
4 help (within the meaning of section 317T) to ASIO in
5 relation to a matter covered by paragraph 317T(2)(a); or
6 (ii) are by way of giving help to ASIO in relation to a
7 matter covered by paragraph 317T(2)(b);
8 the Attorney-General must, within 7 days after extending the
9 period, notify the Inspector-General of Intelligence and Security of
10 the extension.
- 11 (1E) If:
12 (a) the Attorney-General extends the period for which a
13 technical capability notice is in force; and
14 (b) the acts or things specified in the notice:
15 (i) are directed towards ensuring that a designated
16 communications provider is capable of giving listed
17 help (within the meaning of section 317T) to an
18 interception agency in relation to a matter covered by
19 paragraph 317T(2)(a); or
20 (ii) are by way of giving help to an interception agency in
21 relation to a matter covered by paragraph 317T(2)(b);
22 the Attorney-General must, within 7 days after extending the
23 period, notify the Commonwealth Ombudsman of the extension.
- 24 (1F) A failure to comply with subsection (1D) or (1E) does not affect
25 the validity of an extension of a technical capability notice.
- 26 (2) If a technical capability notice expires, this Part does not prevent
27 the giving of a fresh technical capability notice in the same terms
28 as the expired technical capability notice.

29 **317U Compliance period etc.**

- 30 (1) A technical capability notice may require a specified act or thing to
31 be done within a specified period.
- 32 (2) A technical capability notice may require a specified act or thing to
33 be done:
34 (a) in a specified manner; or

1 (b) in a way that meets one or more specified conditions.

2 (3) Subsections (1) and (2) of this section do not limit
3 subsections 317T(1) and (2).

4 **317V Decision-making criteria**

5 The Attorney-General must not give a technical capability notice to
6 a designated communications provider unless:

- 7 (a) the Attorney-General is satisfied that the requirements
8 imposed by the notice are reasonable and proportionate; and
9 (b) the Attorney-General is satisfied that compliance with the
10 notice is:
11 (i) practicable; and
12 (ii) technically feasible.

13 Note: See also section 317ZAA.

14 **317W Consultation about a proposal to give a technical capability
15 notice**

16 (1) The Attorney-General must not give a technical capability notice to
17 a designated communications provider unless the Attorney-General
18 has first:

- 19 (a) given the provider a written notice (the *consultation notice*):
20 (i) setting out a proposal to give the technical capability
21 notice; and
22 (ii) inviting the provider to make a submission to the
23 Attorney-General on the proposed technical capability
24 notice; and
25 (b) considered any submission that was received within the time
26 limit specified in the consultation notice.

27 (2) A time limit specified in a consultation notice must run for at least
28 28 days.

29 (3) The rule in subsection (2) does not apply to a technical capability
30 notice given to a designated communications provider if:
31 (a) the Attorney-General is satisfied that the technical capability
32 notice should be given as a matter of urgency; or
33 (b) compliance with subsection (2) is impracticable; or

- 1 (c) the provider waives compliance with subsection (2).
- 2 (4) For the purposes of paragraph (3)(c), a designated communications
3 provider may waive compliance:
4 (a) orally; or
5 (b) in writing.
- 6 (5) If compliance is waived orally by a designated communications
7 provider, the provider must:
8 (a) make a written record of the waiver; and
9 (b) do so within 48 hours after the waiver was made.
- 10 (6) If, under subsection (5), a designated communications provider
11 makes a written record of the waiver, the provider must:
12 (a) give a copy of the record to the Attorney-General; and
13 (b) do so as soon as practicable after the record was made.
- 14 (7) Subsection (1) does not apply to a technical capability notice
15 proposed to be given to a designated communications provider if:
16 (a) the requirements imposed by the proposed technical
17 capability notice are the same, or substantially the same, as
18 the requirements imposed by another technical capability
19 notice that has previously been given to the provider; and
20 (b) the proposed technical capability notice is to come into force
21 immediately after the expiry of the other technical capability
22 notice.
- 23 *Special consultation requirements for replacement technical*
24 *capability notices*
- 25 (8) Before giving a designated communications provider a technical
26 capability notice that satisfies the following conditions:
27 (a) the requirements imposed by the technical capability notice
28 are the same, or substantially the same, as the requirements
29 imposed by another technical capability notice that has
30 previously been given to the provider;
31 (b) the first-mentioned technical capability notice is to come into
32 force immediately after the expiry of the other technical
33 capability notice;
34 the Attorney-General must consult the provider.
-

- 1 (9) The rule in subsection (8) does not apply to a technical capability
2 notice given to a designated communications provider if the
3 provider waives compliance with subsection (8).

4 **317WA Assessment and report**

5 *Designated communications provider may request carrying out of*
6 *assessment*

- 7 (1) If a consultation notice is given to a designated communications
8 provider under subsection 317W(1) in relation to a proposed
9 technical capability notice, the provider may, within the time limit
10 specified in the consultation notice, give the Attorney-General a
11 written notice requesting the carrying out of an assessment of
12 whether the proposed technical capability notice should be given.

13 *Attorney-General must appoint assessors*

- 14 (2) If a designated communications provider gives the
15 Attorney-General a notice under subsection (1) in relation to a
16 proposed technical capability notice, the Attorney-General must
17 appoint 2 persons to carry out an assessment of whether the
18 proposed technical capability notice should be given.
- 19 (3) For the purposes of this section, the persons appointed under
20 subsection (2) are to be known as the *assessors*.
- 21 (4) One of the assessors must be a person who:
22 (a) has knowledge that would enable the person to assess
23 whether proposed technical capability notices would
24 contravene section 317ZG; and
25 (b) is cleared for security purposes to:
26 (i) the highest level required by staff members of ASIO; or
27 (ii) such lower level as the Attorney-General approves.
- 28 (5) One of the assessors must be a person who:
29 (a) has served as a judge in one or more prescribed courts for a
30 period of 5 years; and
31 (b) no longer holds a commission as a judge of a prescribed
32 court.

1

Assessment and report by assessors

2

(6) As soon as practicable after being appointed under subsection (2),
the assessors must:

3

4

(a) carry out an assessment of whether the proposed technical
capability notice should be given; and

5

6

(b) prepare a report of the assessment; and

7

(c) give a copy of the report to:

8

(i) the Attorney-General; and

9

(ii) the designated communications provider concerned; and

10

(d) if the acts or things specified in the proposed technical
capability notice:

11

12

(i) are directed towards ensuring that the designated
communications provider is capable of giving listed

13

14

help (within the meaning of section 317T) to ASIO in
relation to a matter covered by paragraph 317T(2)(a); or

15

16

(ii) are by way of giving help to ASIO in relation to a
matter covered by paragraph 317T(2)(b);

17

give a copy of the report to the Inspector-General of
Intelligence and Security; and

18

19

(e) if the acts or things specified in the proposed technical
capability notice:

20

21

(i) are directed towards ensuring that the designated
communications provider is capable of giving listed

22

23

help (within the meaning of section 317T) to an

24

25

interception agency in relation to a matter covered by
paragraph 317T(2)(a); or

26

27

(ii) are by way of giving help to an interception agency in
relation to a matter covered by paragraph 317T(2)(b);

28

29

give a copy of the report to the Commonwealth Ombudsman.

30

(7) In carrying out an assessment under paragraph (6)(a) in relation to
a technical capability notice proposed to be given to a designated
communications provider, the assessors must:

31

32

(a) consider:

33

34

(i) whether the proposed technical capability notice would
contravene section 317ZG; and

35

- 1 (ii) whether the requirements imposed by the proposed
2 technical capability notice are reasonable and
3 proportionate; and
4 (iii) whether compliance with the proposed technical
5 capability notice is practicable; and
6 (iv) whether compliance with the proposed technical
7 capability notice is technically feasible; and
8 (v) whether the proposed technical capability notice is the
9 least intrusive measure that would be effective in
10 achieving the legitimate objective of the proposed
11 technical capability notice; and
12 (b) give the greatest weight to the matter mentioned in
13 subparagraph (a)(i).
- 14 (8) In carrying out an assessment under paragraph (6)(a) in relation to
15 a technical capability notice proposed to be given to a designated
16 communications provider, the assessors must consult:
17 (a) the provider; and
18 (b) if the acts or things specified in the proposed technical
19 capability notice:
20 (i) are directed towards ensuring that a designated
21 communications provider is capable of giving listed
22 help (within the meaning of section 317T) to ASIO in
23 relation to a matter covered by paragraph 317T(2)(a); or
24 (ii) are by way of giving help to ASIO in relation to a
25 matter covered by paragraph 317T(2)(b);
26 the Director-General of Security; and
27 (c) if the acts or things specified in the proposed technical
28 capability notice:
29 (i) are directed towards ensuring that a designated
30 communications provider is capable of giving listed
31 help (within the meaning of section 317T) to an
32 interception agency in relation to a matter covered by
33 paragraph 317T(2)(a); or
34 (ii) are by way of giving help to an interception agency in
35 relation to a matter covered by paragraph 317T(2)(b);
36 the chief officer of the interception agency.
- 37 (9) If:
-

- 1 (a) the assessors have begun to carry out an assessment under
2 paragraph (6)(a) in relation to a technical capability notice
3 proposed to be given to a designated communications
4 provider; and
5 (b) the provider informs the Attorney-General that the provider
6 no longer wants the assessment to be carried out;
7 then:
8 (c) the Attorney-General must direct the assessors to cease
9 carrying out the assessment; and
10 (d) the assessors must comply with the direction.

11 (10) If:

- 12 (a) the assessors have begun to carry out an assessment under
13 paragraph (6)(a); and
14 (b) the Attorney-General withdraws the proposed technical
15 capability notice to which the assessment relates;
16 then:
17 (c) the Attorney-General must direct the assessors to cease
18 carrying out the assessment; and
19 (d) the assessors must comply with the direction.

20 *Attorney-General must have regard to the report of the assessment*

21 (11) If:

- 22 (a) a notice is given under subsection (1) in relation to a
23 technical capability notice proposed to be given to a
24 designated communications provider; and
25 (b) a copy of the report relating to the proposed technical
26 capability notice is given to the Attorney-General under
27 subsection (6);
28 the Attorney-General, in considering whether to proceed to give
29 the technical capability notice, must have regard to the copy of the
30 report.

31 *Technical capability notice information*

32 (12) For the purposes of this Part:

- 33 (a) information about the carrying out of an assessment under
34 subsection (6); or

- 1 (b) information contained in a report prepared under
2 subsection (6);
3 is taken to be information about consultation relating to the giving
4 of a technical capability notice.

5 *Prescribed court*

- 6 (13) For the purposes of this section, *prescribed court* means:
7 (a) the High Court; or
8 (b) the Federal Court of Australia; or
9 (c) the Supreme Court of a State or Territory; or
10 (d) the District Court (or equivalent) of a State or Territory.

11 **317X Variation of technical capability notices**

- 12 (1) If a technical capability notice has been given to a designated
13 communications provider, the Attorney-General may, by written
14 notice given to the provider, vary the notice.

15 *Acts or things specified in a varied technical capability notice*

- 16 (2) The acts or things specified in a varied technical capability notice
17 must be:
18 (a) in connection with any or all of the eligible activities of the
19 designated communications provider concerned; and
20 (b) covered by subsection 317T(2).
21 (3) The acts or things specified in a varied technical capability notice
22 in accordance with paragraph 317T(2)(b) must be listed acts or
23 things, so long as those acts or things:
24 (a) are in connection with any or all of the eligible activities of
25 the designated communications provider concerned; and
26 (b) are covered by subsection 317T(2), so far as that subsection
27 relates to paragraph 317T(2)(b).

28 Note: For *listed acts or things*, see section 317E.

29 *Decision-making criteria*

- 30 (4) The Attorney-General must not vary a technical capability notice
31 unless the Attorney-General is satisfied that:
-

- 1 (a) the requirements imposed by the varied notice are reasonable
2 and proportionate; and
3 (b) compliance with the varied notice is:
4 (i) practicable; and
5 (ii) technically feasible.

6 Note: See also section 317ZAA.

7 *Variation must not extend duration of technical capability notice*

- 8 (5) A variation of a technical capability notice must not extend the
9 period for which the notice is in force.

10 *Notification obligations*

- 11 (6) If:
12 (a) the Attorney-General varies a technical capability notice; and
13 (b) the acts or things specified in the varied notice:
14 (i) are directed towards ensuring that a designated
15 communications provider is capable of giving listed
16 help (within the meaning of section 317T) to ASIO in
17 relation to a matter covered by paragraph 317T(2)(a); or
18 (ii) are by way of giving help to ASIO in relation to a
19 matter covered by paragraph 317T(2)(b);
20 the Attorney-General must, within 7 days after varying the notice,
21 notify the Inspector-General of Intelligence and Security that the
22 notice has been varied.

- 23 (7) If:
24 (a) the Attorney-General varies a technical capability notice; and
25 (b) the acts or things specified in the varied notice:
26 (i) are directed towards ensuring that a designated
27 communications provider is capable of giving listed
28 help (within the meaning of section 317T) to an
29 interception agency in relation to a matter covered by
30 paragraph 317T(2)(a); or
31 (ii) are by way of giving help to an interception agency in
32 relation to a matter covered by paragraph 317T(2)(b);

1 the Attorney-General must, within 7 days after varying the notice,
2 notify the Commonwealth Ombudsman that the notice has been
3 varied.

4 (8) A failure to comply with subsection (6) or (7) does not affect the
5 validity of a variation of a technical capability notice.

6 **317XA Approval of variation of technical capability notice**

- 7 (1) If a technical capability notice has been given to a designated
8 communications provider, the Attorney-General must not vary the
9 notice unless:
10 (a) both:
11 (i) the Attorney-General has given the Minister a written
12 notice setting out a proposal to vary the technical
13 capability notice; and
14 (ii) the Minister has approved the variation of the technical
15 capability notice; or
16 (b) the provider has waived compliance with subsection 317Y(2)
17 in relation to the variation of the technical capability notice.
- 18 (2) An approval under subparagraph (1)(a)(ii) may be given:
19 (a) orally; or
20 (b) in writing.
- 21 (3) If an approval under subparagraph (1)(a)(ii) is given orally, the
22 Minister must:
23 (a) make a written record of the approval; and
24 (b) do so within 48 hours after the approval was given.
- 25 (4) The Attorney-General may make a representation to the Minister
26 about the proposal to vary the technical capability notice.
- 27 (5) A representation may deal with:
28 (a) any of the matters set out in section 317ZAA; and
29 (b) such other matters (if any) as the Attorney-General considers
30 relevant.
- 31 (6) In considering whether to approve the variation of the technical
32 capability notice, the Minister must have regard to the following
33 matters:
-

- 1 (a) the objectives of the notice as proposed to be varied;
2 (b) the legitimate interests of the designated communications
3 provider to whom the notice relates;
4 (c) the impact of the notice as proposed to be varied on the
5 efficiency and international competitiveness of the Australian
6 telecommunications industry;
7 (d) the representation (if any) that was made under
8 subsection (4);
9 (e) such other matters (if any) as the Minister considers relevant.

10 **317Y Consultation about a proposal to vary a technical capability**
11 **notice**

- 12 (1) If a technical capability notice has been given to a designated
13 communications provider, the Attorney-General must not vary the
14 notice unless the Attorney-General has first:
15 (a) given the provider a written notice (the *consultation notice*):
16 (i) setting out a proposal to vary the technical capability
17 notice; and
18 (ii) inviting the provider to make a submission to the
19 Attorney-General on the proposed variation; and
20 (b) considered any submission that was received within the time
21 limit specified in the consultation notice.
- 22 (2) A time limit specified in a consultation notice must run for at least
23 28 days.
- 24 (3) If a technical capability notice has been given to a designated
25 communications provider, the rule in subsection (2) does not apply
26 to a variation of the notice if:
27 (a) the Attorney-General is satisfied that the technical capability
28 notice should be varied as a matter of urgency; or
29 (b) compliance with subsection (2) is impracticable; or
30 (c) the provider waives compliance with subsection (2).
- 31 (4) For the purposes of paragraph (3)(c), a designated communications
32 provider may waive compliance:
33 (a) orally; or
34 (b) in writing.

- 1 (5) If compliance is waived orally by a designated communications
2 provider, the provider must:
3 (a) make a written record of the waiver; and
4 (b) do so within 48 hours after the waiver was made.
- 5 (6) If, under subsection (5), a designated communications provider
6 makes a written record of the waiver, the provider must:
7 (a) give a copy of the record to the Attorney-General; and
8 (b) do so as soon as practicable after the record was made.

9 **317YA Assessment and report**

10 *Designated communications provider may request carrying out of*
11 *assessment*

- 12 (1) If:
13 (a) a consultation notice is given to a designated
14 communications provider under subsection 317Y(1) in
15 relation to a proposed variation of a technical capability
16 notice; and
17 (b) the variation is not of a minor nature;
18 the provider may, within the time limit specified in the consultation
19 notice, give the Attorney-General a written notice requesting the
20 carrying out of an assessment of whether the technical capability
21 notice as proposed to be varied would contravene section 317ZG.

22 *Attorney-General must appoint assessors*

- 23 (2) If a designated communications provider gives the
24 Attorney-General a notice under subsection (1) in relation to a
25 technical capability notice as proposed to be varied, the
26 Attorney-General must appoint 2 persons to carry out an
27 assessment of whether the technical capability notice as proposed
28 to be varied would contravene section 317ZG.
- 29 (3) For the purposes of this section, the persons appointed under
30 subsection (2) are to be known as the *assessors*.
- 31 (4) One of the assessors must be a person who:

- 1 (a) has knowledge that would enable the person to assess
2 whether proposed technical capability notices would
3 contravene section 317ZG; and
4 (b) is cleared for security purposes to:
5 (i) the highest level required by staff members of ASIO; or
6 (ii) such lower level as the Attorney-General approves.
- 7 (5) One of the assessors must be a person who:
8 (a) has served as a judge in one or more prescribed courts for a
9 period of 5 years; and
10 (b) no longer holds a commission as a judge of a prescribed
11 court.

12 *Assessment and report by assessors*

- 13 (6) As soon as practicable after being appointed under subsection (2),
14 the assessors must:
15 (a) carry out an assessment of whether the technical capability
16 notice as proposed to be varied would contravene
17 section 317ZG; and
18 (b) prepare a report of the assessment; and
19 (c) give a copy of the report to:
20 (i) the Attorney-General; and
21 (ii) the designated communications provider concerned; and
22 (d) if the acts or things specified in the technical capability
23 notice as proposed to be varied:
24 (i) are directed towards ensuring that the designated
25 communications provider is capable of giving listed
26 help (within the meaning of section 317T) to ASIO in
27 relation to a matter covered by paragraph 317T(2)(a); or
28 (ii) are by way of giving help to ASIO in relation to a
29 matter covered by paragraph 317T(2)(b);
30 give a copy of the report to the Inspector-General of
31 Intelligence and Security; and
32 (e) if the acts or things specified in the technical capability
33 notice as proposed to be varied:
34 (i) are directed towards ensuring that the designated
35 communications provider is capable of giving listed
36 help (within the meaning of section 317T) to an
-

- 1 interception agency in relation to a matter covered by
2 paragraph 317T(2)(a); or
3 (ii) are by way of giving help to an interception agency in
4 relation to a matter covered by paragraph 317T(2)(b);
5 give a copy of the report to the Commonwealth Ombudsman.
- 6 (7) In carrying out an assessment under paragraph (6)(a) in relation to
7 a technical capability notice as proposed to be varied, the assessors
8 must consult:
- 9 (a) the designated communications provider concerned; and
10 (b) if the acts or things specified in the technical capability
11 notice as proposed to be varied:
- 12 (i) are directed towards ensuring that the designated
13 communications provider is capable of giving listed
14 help (within the meaning of section 317T) to ASIO in
15 relation to a matter covered by paragraph 317T(2)(a); or
16 (ii) are by way of giving help to ASIO in relation to a
17 matter covered by paragraph 317T(2)(b);
18 the Director-General of Security; and
- 19 (c) if the acts or things specified in the technical capability
20 notice as proposed to be varied:
- 21 (i) are directed towards ensuring that the designated
22 communications provider is capable of giving listed
23 help (within the meaning of section 317T) to an
24 interception agency in relation to a matter covered by
25 paragraph 317T(2)(a); or
26 (ii) are by way of giving help to an interception agency in
27 relation to a matter covered by paragraph 317T(2)(b);
28 the chief officer of the interception agency.
- 29 (8) If:
- 30 (a) the assessors have begun to carry out an assessment under
31 paragraph (6)(a) in relation to the technical capability notice
32 as proposed to be varied; and
33 (b) the designated communications provider concerned informs
34 the Attorney-General that the provider no longer wants the
35 assessment to be carried out;
- 36 then:

- 1 (c) the Attorney-General must direct the assessors to cease
2 carrying out the assessment; and
3 (d) the assessors must comply with the direction.

4 (9) If:

- 5 (a) the assessors have begun to carry out an assessment under
6 paragraph (6)(a); and
7 (b) the Attorney-General withdraws the proposed variation of the
8 technical capability notice concerned;

9 then:

- 10 (c) the Attorney-General must direct the assessors to cease
11 carrying out the assessment; and
12 (d) the assessors must comply with the direction.

13 *Attorney-General must have regard to the report of the assessment*

14 (10) If:

- 15 (a) a notice is given under subsection (1) in relation to a
16 proposed variation of a technical capability notice; and
17 (b) a copy of the report relating to the technical capability notice
18 as proposed to be varied is given to the Attorney-General
19 under subsection (6);

20 the Attorney-General, in considering whether to proceed to vary
21 the technical capability notice, must have regard to the copy of the
22 report.

23 *Technical capability notice information*

24 (11) For the purposes of this Part:

- 25 (a) information about the carrying out of an assessment under
26 subsection (6); or
27 (b) information contained in a report prepared under
28 subsection (6);

29 is taken to be information about consultation relating to the
30 variation of a technical capability notice.

31 *Prescribed court*

32 (12) For the purposes of this section, *prescribed court* means:

- 33 (a) the High Court; or
-

- 1 (b) the Federal Court of Australia; or
2 (c) the Supreme Court of a State or Territory; or
3 (d) the District Court (or equivalent) of a State or Territory.

4 **317Z Revocation of technical capability notices**

- 5 (1) If a technical capability notice has been given to a person, the
6 Attorney-General may, by written notice given to the person,
7 revoke the notice.
- 8 (2) If a technical capability notice has been given to a person, and the
9 Attorney-General is satisfied that:
10 (a) the requirements imposed by the notice are not reasonable
11 and proportionate; or
12 (b) compliance with the notice is not:
13 (i) practicable; and
14 (ii) technically feasible;
15 the Attorney-General must, by written notice given to the person,
16 revoke the notice.

17 *Notification obligations*

- 18 (3) If:
19 (a) the Attorney-General revokes a technical capability notice;
20 and
21 (b) the acts or things specified in the revoked notice:
22 (i) are directed towards ensuring that a designated
23 communications provider is capable of giving listed
24 help (within the meaning of section 317T) to ASIO in
25 relation to a matter covered by paragraph 317T(2)(a); or
26 (ii) are by way of giving help to ASIO in relation to a
27 matter covered by paragraph 317T(2)(b);
28 the Attorney-General must, within 7 days after revoking the notice,
29 notify the Inspector-General of Intelligence and Security that the
30 notice has been revoked.
- 31 (4) If:
32 (a) the Attorney-General revokes a technical capability notice;
33 and

- 1 (b) the acts or things specified in the revoked notice:
2 (i) are directed towards ensuring that a designated
3 communications provider is capable of giving listed
4 help (within the meaning of section 317T) to an
5 interception agency in relation to a matter covered by
6 paragraph 317T(2)(a); or
7 (ii) are by way of giving help to an interception agency in
8 relation to a matter covered by paragraph 317T(2)(b);
9 the Attorney-General must, within 7 days after revoking the notice,
10 notify the Commonwealth Ombudsman that the notice has been
11 revoked.
- 12 (5) A failure to comply with subsection (3) or (4) does not affect the
13 validity of a revocation of a technical capability notice.

14 **317ZAA Whether requirements imposed by a technical capability**
15 **notice are reasonable and proportionate**

- 16 In considering whether the requirements imposed by a technical
17 capability notice or a varied technical capability notice are
18 reasonable and proportionate, the Attorney-General must have
19 regard to the following matters:
- 20 (a) the interests of national security;
21 (b) the interests of law enforcement;
22 (c) the legitimate interests of the designated communications
23 provider to whom the notice relates;
24 (d) the objectives of the notice;
25 (e) the availability of other means to achieve the objectives of
26 the notice;
- 27 (ea) whether the requirements, when compared to other forms of
28 industry assistance known to the Attorney-General, are the
29 least intrusive form of industry assistance so far as the
30 following persons are concerned:
31 (i) persons whose activities are not of interest to ASIO;
32 (ii) persons whose activities are not of interest to
33 interception agencies;
- 34 (eb) whether the requirements are necessary;
35 (f) the legitimate expectations of the Australian community
36 relating to privacy and cybersecurity;
-

- 1 (g) such other matters (if any) as the Attorney-General considers
2 relevant.

3 **Division 5—Compliance and enforcement**

4 **317ZA Compliance with notices—carriers and carriage service**
5 **providers**

- 6 (1) A carrier or carriage service provider must comply with a
7 requirement under:
8 (a) a technical assistance notice; or
9 (b) a technical capability notice;
10 to the extent that the carrier or provider is capable of doing so.
- 11 (2) A person must not:
12 (a) aid, abet, counsel or procure a contravention of
13 subsection (1); or
14 (b) induce, whether by threats or promises or otherwise, a
15 contravention of subsection (1); or
16 (c) be in any way, directly or indirectly, knowingly concerned in,
17 or party to, a contravention of subsection (1); or
18 (d) conspire with others to effect a contravention of
19 subsection (1).
- 20 (3) Subsections (1) and (2) are civil penalty provisions.
- 21 Note: Part 31 provides for pecuniary penalties for breaches of civil penalty
22 provisions.

23 **317ZB Compliance with notices—designated communications**
24 **provider (other than a carrier or carriage service**
25 **provider)**

- 26 (1) A designated communications provider (other than a carrier or
27 carriage service provider) must comply with a requirement under:
28 (a) a technical assistance notice; or
29 (b) a technical capability notice;
30 to the extent that the provider is capable of doing so.
- 31 Civil penalty:

- 1 (a) if the provider is a body corporate—47,619 penalty units; or
2 (b) if the provider is not a body corporate—238 penalty units.
- 3 (2) The pecuniary penalty for a contravention by a designated
4 communications provider of subsection (1) must not be more than:
5 (a) if the provider is a body corporate—47,619 penalty units; or
6 (b) if the provider is not a body corporate—238 penalty units.
- 7 (3) Subsection 82(5) of the *Regulatory Powers (Standard Provisions)*
8 *Act 2014* does not apply to a contravention of subsection (1) of this
9 section.
- 10 (4) Sections 564 and 572B do not apply to a contravention of
11 subsection (1) of this section.
- 12 (5) In proceedings for a civil penalty order against a designated
13 communications provider for a contravention of subsection (1) in
14 relation to:
15 (a) a requirement under a technical assistance notice to do an act
16 or thing in a foreign country; or
17 (b) a requirement under a technical capability notice to do an act
18 or thing in a foreign country;
19 it is a defence if the provider proves that compliance with the
20 requirement in the foreign country would contravene a law of the
21 foreign country.

22 **317ZC Civil penalty provision**

23 *Enforceable civil penalty provision*

- 24 (1) Section 317ZB of this Act is enforceable under Part 4 of the
25 *Regulatory Powers (Standard Provisions) Act 2014*.

26 Note: Part 4 of the *Regulatory Powers (Standard Provisions) Act 2014*
27 allows a civil penalty provision to be enforced by obtaining an order
28 for a person to pay a pecuniary penalty for the contravention of the
29 provision.

1 *Authorised applicant*

- 2 (2) For the purposes of Part 4 of the *Regulatory Powers (Standard*
3 *Provisions) Act 2014*, the Communications Access Co-ordinator is
4 an authorised applicant in relation to section 317ZB of this Act.

5 *Relevant courts*

- 6 (3) For the purposes of Part 4 of the *Regulatory Powers (Standard*
7 *Provisions) Act 2014*, the Federal Court and the Federal Circuit
8 Court of Australia are relevant courts in relation to section 317ZB
9 of this Act.

10 *Extension to external Territories etc.*

- 11 (4) Part 4 of the *Regulatory Powers (Standard Provisions) Act 2014*,
12 as it applies in relation to section 317ZB of this Act, extends to:
13 (a) every external Territory; and
14 (b) acts, omissions, matters and things outside Australia.

15 **317ZD Enforceable undertakings**

16 *Enforceable provision*

- 17 (1) Section 317ZB of this Act is enforceable under Part 6 of the
18 *Regulatory Powers (Standard Provisions) Act 2014*.

19 *Authorised person*

- 20 (2) The Communications Access Co-ordinator is an authorised person
21 in relation to section 317ZB of this Act for the purposes of Part 6
22 of the *Regulatory Powers (Standard Provisions) Act 2014*.

23 *Relevant courts*

- 24 (3) The Federal Court and the Federal Circuit Court of Australia are
25 relevant courts in relation to section 317ZB of this Act for the
26 purposes of Part 6 of the *Regulatory Powers (Standard Provisions)*
27 *Act 2014*.

1 *Extension to external Territories etc.*

- 2 (4) Part 6 of the *Regulatory Powers (Standard Provisions) Act 2014*,
3 as it applies in relation to section 317ZB of this Act, extends to:
4 (a) every external Territory; and
5 (b) acts, omissions, matters and things outside Australia.

6 **317ZE Injunctions**

7 *Enforceable provision*

- 8 (1) Section 317ZB of this Act is enforceable under Part 7 of the
9 *Regulatory Powers (Standard Provisions) Act 2014*.

10 *Authorised person*

- 11 (2) The Communications Access Co-ordinator is an authorised person
12 in relation to section 317ZB of this Act for the purposes of Part 7
13 of the *Regulatory Powers (Standard Provisions) Act 2014*.

14 *Relevant courts*

- 15 (3) The Federal Court and the Federal Circuit Court of Australia are
16 relevant courts in relation to section 317ZB of this Act for the
17 purposes of Part 7 of the *Regulatory Powers (Standard Provisions)*
18 *Act 2014*.

19 *Extension to external Territories etc.*

- 20 (4) Part 7 of the *Regulatory Powers (Standard Provisions) Act 2014*,
21 as it applies in relation to section 317ZB of this Act, extends to:
22 (a) every external Territory; and
23 (b) acts, omissions, matters and things outside Australia.

24 **Division 6—Unauthorised disclosure of information etc.**

25 **317ZF Unauthorised disclosure of information**

- 26 (1) A person commits an offence if:
27 (a) the person discloses information; and
28 (b) the person is or was:
-

Schedule 1 Industry assistance
Part 1 Amendments

- 1 (i) a designated communications provider; or
2 (ii) an employee of a designated communications provider;
3 or
4 (iii) a contracted service provider of a designated
5 communications provider; or
6 (iv) an employee of a contracted service provider of a
7 designated communications provider; or
8 (v) an entrusted ASIO person; or
9 (vi) an entrusted ASIS person; or
10 (vii) an entrusted ASD person; or
11 (viii) an officer of an interception agency; or
12 (ix) an officer or employee of the Commonwealth, a State or
13 a Territory; or
14 (x) a person appointed under subsection 317WA(2); or
15 (xa) a person appointed under subsection 317YA(2); or
16 (xi) an arbitrator appointed under section 317ZK; and
17 (c) the information:
18 (i) is technical assistance notice information; or
19 (ii) is technical capability notice information; or
20 (iii) is technical assistance request information; or
21 (iv) was obtained in accordance with a technical assistance
22 notice; or
23 (v) was obtained in accordance with a technical capability
24 notice; or
25 (vi) was obtained in accordance with a technical assistance
26 request; and
27 (d) if the information is covered by subparagraph (c)(i), (ii) or
28 (iii)—the information has come to the person’s knowledge,
29 or into the person’s possession:
30 (i) if the person is or was a designated communications
31 provider—in connection with the person’s capacity as
32 such a provider; or
33 (ii) if the person is or was an employee of a designated
34 communications provider—because the person is or was
35 employed by the provider in connection with its
36 business as such a provider; or

- 1 (iii) if the person is or was a contracted service provider of a
2 designated communications provider—in connection
3 with the person’s business as such a contracted service
4 provider; or
5 (iv) if the person is or was an employee of a contracted
6 service provider of a designated communications
7 provider—because the person is or was employed by the
8 contractor in connection with its business as such a
9 contracted service provider; or
10 (v) if the person is or was an entrusted ASIO person—in the
11 person’s capacity as such an entrusted ASIO person; or
12 (vi) if the person is or was an entrusted ASIS person—in the
13 person’s capacity as such an entrusted ASIS person; or
14 (vii) if the person is or was an entrusted ASD person—in the
15 person’s capacity as such an entrusted ASD person; or
16 (viii) if the person is or was an officer of an interception
17 agency—in the person’s capacity as such an officer; or
18 (ix) if the person is or was an officer or employee of the
19 Commonwealth, a State or a Territory—in the person’s
20 capacity as such an officer or employee; or
21 (ixa) if the person is or was a person appointed under
22 subsection 317WA(2)—in the person’s capacity as such
23 an appointee; or
24 (ixb) if the person is or was a person appointed under
25 subsection 317YA(2)—in the person’s capacity as such
26 an appointee; or
27 (x) if the person is or was an arbitrator appointed under
28 section 317ZK—in the person’s capacity as such an
29 arbitrator; and
30 (e) if the information is covered by subparagraph (c)(iv), (v) or
31 (vi)—the information has come to the person’s knowledge, or
32 into the person’s possession:
33 (i) if the person is or was an entrusted ASIO person—in the
34 person’s capacity as such an entrusted ASIO person; or
35 (ii) if the person is or was an entrusted ASIS person—in the
36 person’s capacity as such an entrusted ASIS person; or
37 (iii) if the person is or was an entrusted ASD person—in the
38 person’s capacity as such an entrusted ASD person; or
-

- 1 (iv) if the person is or was an officer of an interception
2 agency—in the person’s capacity as such an officer; or
3 (v) if the person is or was an officer or employee of the
4 Commonwealth, a State or a Territory—in the person’s
5 capacity as such an officer or employee; or
6 (vi) if the person is or was an arbitrator appointed under
7 section 317ZK—in the person’s capacity as such an
8 arbitrator.

9 Penalty: Imprisonment for 5 years.

10 *Exceptions*

- 11 (2) Subsection (1) does not apply if the disclosure was authorised
12 under subsection (3), (5), (5A), (5B), (5C), (6), (7), (8), (9), (10),
13 (11), (12A), (12B), (12C), (12D), (13), (14), (15) or (16).

14 Note: Except as provided by subsection (2A) or (2B), a defendant bears an
15 evidential burden in relation to the matters in this subsection—see
16 subsection 13.3(3) of the *Criminal Code*.

- 17 (2A) Despite subsection 13.3(3) of the *Criminal Code*, in a prosecution
18 for an offence against subsection (1) of this section, an IGIS
19 official does not bear an evidential burden in relation to the matters
20 in subsection (2) of this section, to the extent to which that
21 subsection relates to subsection (5) of this section.

- 22 (2B) Despite subsection 13.3(3) of the *Criminal Code*, in a prosecution
23 for an offence against subsection (1) of this section, an
24 Ombudsman official does not bear an evidential burden in relation
25 to the matters in subsection (2) of this section, to the extent to
26 which that subsection relates to subsection (5A), (5B) or (5C) of
27 this section.

28 *Authorised disclosures—general*

- 29 (3) A person covered by paragraph (1)(b) may disclose technical
30 assistance notice information, technical capability notice
31 information or technical assistance request information:
32 (a) in connection with the administration or execution of this
33 Part; or

- 1 (b) for the purposes of any legal proceedings arising out of or
2 otherwise related to this Part or of any report of any such
3 proceedings; or
4 (c) in accordance with any requirement imposed by a law of the
5 Commonwealth, a State or a Territory; or
6 (d) in connection with the performance of functions, or the
7 exercise of powers, by:
8 (i) ASIO; or
9 (ii) the Australian Secret Intelligence Service; or
10 (iii) the Australian Signals Directorate; or
11 (iv) an interception agency; or
12 (e) for the purpose of obtaining legal advice in relation to this
13 Part; or
14 (f) to an IGIS official for the purpose of exercising powers, or
15 performing functions or duties, as an IGIS official; or
16 (g) to an Ombudsman official for the purpose of exercising
17 powers, or performing functions or duties, as an Ombudsman
18 official.
- 19 (4) For the purposes of subsection (3), **this Part** includes:
20 (a) any other provision of this Act, so far as that other provision
21 relates to this Part; and
22 (b) the *Regulatory Powers (Standard Provisions) Act 2014*, so
23 far as that Act relates to this Part.

24 *Authorised disclosures—IGIS official*

- 25 (5) An IGIS official may disclose:
26 (a) technical assistance notice information; or
27 (b) technical capability notice information; or
28 (c) technical assistance request information;
29 in connection with the IGIS official exercising powers, or
30 performing functions or duties, as an IGIS official.

31 *Authorised disclosures—Ombudsman official*

- 32 (5A) An Ombudsman official may disclose:
33 (a) technical assistance notice information; or
34 (b) technical capability notice information;
-

- 1 (c) technical assistance request information;
2 in connection with the Ombudsman official exercising powers, or
3 performing functions or duties, as an Ombudsman official.
- 4 (5B) If a technical assistance notice is given by the chief officer of an
5 interception agency of a State or Territory, an Ombudsman official
6 may disclose technical assistance notice information that relates to
7 the notice to an officer or employee of an authority that is the State
8 or Territory inspecting authority in relation to the interception
9 agency, so long as the disclosure is in connection with the officer
10 or employee exercising powers, or performing functions or duties,
11 as an officer or employee of the State or Territory inspecting
12 authority.
- 13 (5C) If a technical assistance request is given by the chief officer of an
14 interception agency of a State or Territory, an Ombudsman official
15 may disclose technical assistance request information that relates to
16 the request to an officer or employee of an authority that is the
17 State or Territory inspecting authority in relation to the interception
18 agency, so long as the disclosure is in connection with the officer
19 or employee exercising powers, or performing functions or duties,
20 as an officer or employee of the State or Territory inspecting
21 authority.
- 22 *Authorised disclosures—information sharing*
- 23 (6) The Director-General of Security or the Communications Access
24 Co-ordinator may disclose information that is:
25 (a) technical assistance notice information; or
26 (b) technical capability notice information; or
27 (c) technical assistance request information;
28 to the chief officer of an interception agency for purposes relating
29 to the performance of functions, or the exercise of powers, by the
30 interception agency.
- 31 (7) The chief officer of an interception agency may disclose
32 information that is:
33 (a) technical assistance notice information; or
34 (b) technical capability notice information; or
35 (c) technical assistance request information;
-

1 to the chief officer of another interception agency for purposes
2 relating to the performance of functions, or the exercise of powers,
3 by the other interception agency.

4 (8) The Director-General of Security, the Director-General of the
5 Australian Signals Directorate or the chief officer of an
6 interception agency may disclose information that is:

- 7 (a) technical assistance notice information; or
- 8 (b) technical capability notice information; or
- 9 (c) technical assistance request information;

10 to the Director-General of the Australian Secret Intelligence
11 Service for purposes relating to the performance of functions, or
12 the exercise of powers, by the Australian Secret Intelligence
13 Service.

14 (9) The Director-General of Security, the Director-General of the
15 Australian Secret Intelligence Service or the chief officer of an
16 interception agency may disclose information that is:

- 17 (a) technical assistance notice information; or
- 18 (b) technical capability notice information; or
- 19 (c) technical assistance request information;

20 to the Director-General of the Australian Signals Directorate for
21 purposes relating to the performance of functions, or the exercise
22 of powers, by the Australian Signals Directorate.

23 (10) The Communications Access Co-ordinator, the Director-General of
24 the Australian Secret Intelligence Service, the Director-General of
25 the Australian Signals Directorate or the chief officer of an
26 interception agency may disclose information that is:

- 27 (a) technical assistance notice information; or
- 28 (b) technical capability notice information; or
- 29 (c) technical assistance request information;

30 to the Director-General of Security for purposes relating to the
31 performance of functions, or the exercise of powers, by ASIO.

32 (11) The Director-General of Security or the chief officer of an
33 interception agency may disclose information that is:

- 34 (a) technical assistance notice information; or
- 35 (b) technical capability notice information; or

1 (c) technical assistance request information;
2 to the Communications Access Co-ordinator for purposes relating
3 to the performance of functions, or the exercise of powers, by the
4 Communications Access Co-ordinator.

5 (12) Before disclosing information under subsection (6), (7), (8), (9) or
6 (10), the Director-General of Security, the Director-General of the
7 Australian Secret Intelligence Service, the Director-General of the
8 Australian Signals Directorate or the chief officer of an
9 interception agency, as the case requires, must notify the
10 Communications Access Co-ordinator of the proposed disclosure.

11 *Authorised disclosures—Communications Access Co-ordinator*

12 (12A) If:

13 (a) the Attorney-General has given a technical capability notice;
14 and

15 (b) the acts or things specified in the notice:

16 (i) are directed towards ensuring that a designated
17 communications provider is capable of giving listed
18 help (within the meaning of section 317T) to an
19 interception agency of a State or Territory in relation to
20 a matter covered by paragraph 317T(2)(a); or

21 (ii) are by way of giving help to an interception agency of a
22 State or Territory in relation to a matter covered by
23 paragraph 317T(2)(b);

24 the Communications Access Co-ordinator may disclose technical
25 capability notice information that relates to the notice to an officer
26 or employee of an authority that is the State or Territory inspecting
27 authority in relation to the interception agency, so long as the
28 disclosure is in connection with the officer or employee exercising
29 powers, or performing functions or duties, as an officer or
30 employee of the State or Territory inspecting authority.

31 *Authorised disclosures—State or Territory inspecting authority*

32 (12B) If a technical assistance notice has been given to a designated
33 communications provider by the chief officer of an interception
34 agency of a State or Territory:

35 (a) the designated communications provider; or

- 1 (b) an employee of the designated communications provider; or
2 (c) a contracted service provider of the designated
3 communications provider; or
4 (d) an employee of a contracted service provider of the
5 designated communications provider;
6 may disclose technical assistance notice information that relates to
7 the notice to an officer or employee of an authority that is the State
8 or Territory inspecting authority in relation to the interception
9 agency, so long as the disclosure is in connection with the officer
10 or employee exercising powers, or performing functions or duties,
11 as an officer or employee of the State or Territory inspecting
12 authority.
- 13 (12C) If a technical assistance request has been given to a designated
14 communications provider by the chief officer of an interception
15 agency of a State or Territory:
16 (a) the designated communications provider; or
17 (b) an employee of the designated communications provider; or
18 (c) a contracted service provider of the designated
19 communications provider; or
20 (d) an employee of a contracted service provider of the
21 designated communications provider;
22 may disclose technical assistance request information that relates to
23 the request to an officer or employee of an authority that is the
24 State or Territory inspecting authority in relation to the interception
25 agency, so long as the disclosure is in connection with the officer
26 or employee exercising powers, or performing functions or duties,
27 as an officer or employee of the State or Territory inspecting
28 authority.
- 29 (12D) If:
30 (a) technical assistance notice information is disclosed under
31 subsection (12B); or
32 (b) technical assistance request information is disclosed under
33 subsection (12C);
34 to an officer or employee of an authority that is the State or
35 Territory inspecting authority in relation to an interception agency,
36 the officer or employee may disclose the information in connection
37 with the officer or employee exercising powers, or performing
-

1 functions or duties, as an officer or employee of the State or
2 Territory inspecting authority.

3 *Authorised disclosures—statistics*

4 (13) A person who is:

- 5 (a) a designated communications provider; or
- 6 (b) an employee of a designated communications provider; or
- 7 (c) a contracted service provider of a designated communications
8 provider; or
- 9 (d) an employee of a contracted service provider of a designated
10 communications provider;

11 may, in the person's capacity as such a provider or employee,
12 disclose:

- 13 (e) the total number of technical assistance notices given to the
14 provider during a period of at least 6 months; or
- 15 (f) the total number of technical capability notices given to the
16 provider during a period of at least 6 months; or
- 17 (g) the total number of technical assistance requests given to the
18 provider during a period of at least 6 months.

19 Note: This subsection authorises the disclosure of aggregate statistical
20 information. That information cannot be broken down:

- 21 (a) by agency; or
- 22 (b) in any other way.

23 *Other authorised disclosures*

24 (14) If a technical assistance notice has been given to a designated
25 communications provider by the Director-General of Security, the
26 Director-General of Security may, if requested to do so by the
27 designated communications provider, authorise:

- 28 (a) the designated communications provider; or
- 29 (b) a specified employee of the designated communications
30 provider; or
- 31 (c) a specified contracted service provider of the designated
32 communications provider; or
- 33 (d) a specified employee of a contracted service provider of the
34 designated communications provider;

1 to disclose, in accordance with the conditions specified in the
2 authorisation, specified technical assistance notice information that
3 relates to the notice.

4 (15) If a technical assistance notice has been given to a designated
5 communications provider by the chief officer of an interception
6 agency, the chief officer may, if requested to do so by the
7 designated communications provider, authorise:
8 (a) the designated communications provider; or
9 (b) a specified employee of the designated communications
10 provider; or
11 (c) a specified contracted service provider of the designated
12 communications provider; or
13 (d) a specified employee of a contracted service provider of the
14 designated communications provider;
15 to disclose, in accordance with the conditions specified in the
16 authorisation, specified technical assistance notice information that
17 relates to the notice.

18 (16) If a technical capability notice has been given to a designated
19 communications provider, the Attorney-General may, if requested
20 to do so by the designated communications provider, authorise:
21 (a) the designated communications provider; or
22 (b) a specified employee of the designated communications
23 provider; or
24 (c) a specified contracted service provider of the designated
25 communications provider; or
26 (d) a specified employee of a contracted service provider of the
27 designated communications provider;
28 to disclose, in accordance with the conditions specified in the
29 authorisation, specified technical capability notice information that
30 relates to the notice.

31 (17) An authorisation under subsection (14), (15) or (16) must be in
32 writing.

33 **317ZFA Powers of a court**

34 (1) In a proceeding under, or arising out of:
35 (a) this Part; or

- 1 (b) any other provision of this Act, so far as that other provision
2 relates to this Part; or
3 (c) the *Regulatory Powers (Standard Provisions) Act 2014*, so
4 far as that Act relates to this Part;
5 a court may make such orders as the court considers appropriate in
6 relation to the disclosure, protection, storage, handling or
7 destruction, in the proceeding, of:
8 (d) technical assistance notice information; or
9 (e) technical capability notice information; or
10 (f) technical assistance request information;
11 if the court is satisfied that it is in the public interest to make such
12 orders.
- 13 (2) The powers conferred on a court by subsection (1) are in addition
14 to any other powers of the court.

15 Division 7—Limitations

16 **317ZG Designated communications provider must not be requested 17 or required to implement or build a systemic weakness or 18 systemic vulnerability etc.**

- 19 (1) A technical assistance request, technical assistance notice or
20 technical capability notice must not have the effect of:
21 (a) requesting or requiring a designated communications
22 provider to implement or build a systemic weakness, or a
23 systemic vulnerability, into a form of electronic protection; or
24 (b) preventing a designated communications provider from
25 rectifying a systemic weakness, or a systemic vulnerability,
26 in a form of electronic protection.
- 27 (2) The reference in paragraph (1)(a) to implement or build a systemic
28 weakness, or a systemic vulnerability, into a form of electronic
29 protection includes a reference to implement or build a new
30 decryption capability in relation to a form of electronic protection.
- 31 (3) The reference in paragraph (1)(a) to implement or build a systemic
32 weakness, or a systemic vulnerability, into a form of electronic
33 protection includes a reference to one or more actions that would

- 1 render systemic methods of authentication or encryption less
2 effective.
- 3 (4) Subsections (2) and (3) are enacted for the avoidance of doubt.
- 4 (4A) In a case where a weakness is selectively introduced to one or more
5 target technologies that are connected with a particular person, the
6 reference in paragraph (1)(a) to implement or build a systemic
7 weakness into a form of electronic protection includes a reference
8 to any act or thing that will, or is likely to, jeopardise the security
9 of any information held by any other person.
- 10 (4B) In a case where a vulnerability is selectively introduced to one or
11 more target technologies that are connected with a particular
12 person, the reference in paragraph (1)(a) to implement or build a
13 systemic vulnerability into a form of electronic protection includes
14 a reference to any act or thing that will, or is likely to, jeopardise
15 the security of any information held by any other person.
- 16 (4C) For the purposes of subsections (4A) and (4B), an act or thing will,
17 or is likely to, jeopardise the security of information if the act or
18 thing creates a material risk that otherwise secure information can
19 be accessed by an unauthorised third party.
- 20 (5) A technical assistance request, technical assistance notice or
21 technical capability notice has no effect to the extent (if any) to
22 which it would have an effect covered by paragraph (1)(a) or (b).

23 **317ZGA Limits on technical capability notices**

- 24 (1) If:
- 25 (a) a designated communications provider supplies a particular
26 kind of telecommunications service; and
- 27 (b) the service involves, or will involve, the use of a
28 telecommunications system;
- 29 a technical capability notice has no effect to the extent (if any) to
30 which it requires the provider to ensure that the kind of service, or
31 the system:
- 32 (c) has the capability to enable a communication passing over
33 the system to be intercepted in accordance with an
34 interception warrant; or

Schedule 1 Industry assistance
Part 1 Amendments

1 (d) has the capability to transmit lawfully intercepted
2 information to the delivery points applicable in respect of that
3 kind of service; or

4 (e) has a delivery capability.

5 Note 1: Part 5-3 of the *Telecommunications (Interception and Access) Act*
6 *1979* deals with interception capability.

7 Note 2: Part 5-5 of the *Telecommunications (Interception and Access) Act*
8 *1979* deals with delivery capability.

9 (2) For the purposes of subsection (1), ensuring that a kind of service
10 or a system has a particular capability includes ensuring that the
11 capability is developed, installed and maintained.

12 (3) A technical capability notice has no effect to the extent (if any) to
13 which it requires a designated communications provider to keep, or
14 cause to be kept:

15 (a) information of a kind specified in or under section 187AA of
16 the *Telecommunications (Interception and Access) Act 1979*;
17 or

18 (b) documents containing information of that kind;

19 relating to any communication carried by means of a service to
20 which Part 5-1A of the *Telecommunications (Interception and*
21 *Access) Act 1979* applies.

22 Note: Part 5-1A of the *Telecommunications (Interception and Access) Act*
23 *1979* deals with data retention.

24 (4) A technical capability notice has no effect to the extent (if any) to
25 which it requires a designated communications provider to keep, or
26 cause to be kept, information that:

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

30 (b) was obtained by the provider only as a result of providing the
31 service.

32 Note: This subsection ensures that a technical capability notice cannot
33 require a designated communications provider to keep information
34 about subscribers' web browsing history.

- 1 (5) An expression used in this section and in Chapter 5 of the
2 *Telecommunications (Interception and Access) Act 1979* has the
3 same meaning in this section as it has in that Chapter.

4 **317ZH General limits on technical assistance requests, technical**
5 **assistance notices and technical capability notices**

- 6 (1) A technical assistance request that relates to an agency, or a
7 technical assistance notice that relates to an agency, or a technical
8 capability notice that relates to an agency, has no effect to the
9 extent (if any) to which it would request or require a designated
10 communications provider to do an act or thing for which the
11 agency, or an officer of the agency, would be required to have or
12 obtain a warrant or authorisation under any of the following laws:
13 (a) the *Telecommunications (Interception and Access) Act 1979*;
14 (b) the *Surveillance Devices Act 2004*;
15 (c) the *Crimes Act 1914*;
16 (d) the *Australian Security Intelligence Organisation Act 1979*;
17 (f) a law of the Commonwealth (other than this Part) that is not
18 covered by paragraph (a), (b), (c) or (d);
19 (g) a law of a State or Territory.
- 20 (2) For the purposes of subsection (1):
21 (a) assume that each law mentioned in that subsection applied
22 both within and outside Australia; and
23 (b) assume that each reference in Part 13 to a carriage service
24 provider included a reference to a designated
25 communications provider.
- 26 (3) A technical assistance request, technical assistance notice or
27 technical capability notice has no effect to the extent (if any) to
28 which it would request or require a designated communications
29 provider to:
30 (a) use a surveillance device (within the meaning of the
31 *Surveillance Devices Act 2004*); or
32 (b) access data held in a computer (within the meaning of the
33 *Surveillance Devices Act 2004*);
34 if a law of a State or Territory requires a warrant or authorisation
35 for that use or access.

- 1 (4) To avoid doubt, subsection (1) or (3) does not prevent a technical
2 assistance request, technical assistance notice or technical
3 capability notice from requesting or requiring a designated
4 communications provider to do an act or thing by way of giving
5 help to:
6 (a) ASIO; or
7 (b) an interception agency;
8 in relation to:
9 (ca) in the case of a technical assistance request—a matter
10 covered by subparagraph 317G(2)(b)(v) or (vi); or
11 (c) in the case of a technical assistance notice—a matter covered
12 by paragraph 317L(2)(c) or (d); or
13 (d) in the case of a technical capability notice—a matter covered
14 by subparagraph 317T(2)(b)(i) or (ii);
15 if the doing of the act or thing would:
16 (e) assist in, or facilitate, giving effect to a warrant or
17 authorisation under a law of the Commonwealth, a State or a
18 Territory; or
19 (f) give effect to a warrant or authorisation under a law of the
20 Commonwealth.
- 21 (5) To avoid doubt, subsection (1) or (3) does not prevent a technical
22 capability notice from requiring a designated communications
23 provider to do an act or thing directed towards ensuring that the
24 provider is capable of giving listed help (within the meaning of
25 section 317T) to:
26 (a) ASIO; or
27 (b) an interception agency;
28 in relation to a matter covered by subparagraph 317T(2)(a)(i) or
29 (ii), if the doing of the act or thing would:
30 (c) assist in, or facilitate, giving effect to a warrant or
31 authorisation under a law of the Commonwealth, a State or a
32 Territory; or
33 (d) give effect to a warrant or authorisation under a law of the
34 Commonwealth.

1 *Interpretation*

- 2 (6) For the purposes of this section, a technical assistance request
3 **relates to** an agency if:
4 (a) if the agency is ASIO—the request was given by the
5 Director-General of Security; or
6 (b) if the agency is the Australian Secret Intelligence Service—
7 the request was given by the Director-General of the
8 Australian Secret Intelligence Service; or
9 (c) if the agency is the Australian Signals Directorate—the
10 request was given by the Director-General of the Australian
11 Signals Directorate; or
12 (d) if the agency is an interception agency—the request was
13 given by the chief officer of the interception agency.
- 14 (7) For the purposes of this section, a technical assistance notice
15 **relates to** an agency if:
16 (a) if the agency is ASIO—the notice was given by the
17 Director-General of Security; or
18 (b) if the agency is an interception agency—the notice was given
19 by the chief officer of the interception agency.
- 20 (8) For the purposes of this section, a technical capability notice
21 **relates to** an agency if:
22 (a) if the agency is ASIO—the acts or things specified in the
23 notice:
24 (i) are directed towards ensuring that a designated
25 communications provider is capable of giving listed
26 help (within the meaning of section 317T) to ASIO in
27 relation to a matter covered by paragraph 317T(2)(a); or
28 (ii) are by way of giving help to ASIO in relation to a
29 matter covered by paragraph 317T(2)(b); or
30 (b) if the agency is an interception agency—the acts or things
31 specified in the notice:
32 (i) are directed towards ensuring that a designated
33 communications provider is capable of giving listed
34 help (within the meaning of section 317T) to the
35 interception agency in relation to a matter covered by
36 paragraph 317T(2)(a); or

- 1 (ii) are by way of giving help to the interception agency in
2 relation to a matter covered by paragraph 317T(2)(b).
- 3 (9) For the purposes of this section, *agency* means:
4 (a) ASIO; or
5 (b) the Australian Secret Intelligence Service; or
6 (c) the Australian Signals Directorate; or
7 (d) an interception agency.
- 8 (10) For the purposes of this section, *officer* of an agency means:
9 (a) if the agency is ASIO:
10 (i) the Director-General of Security; or
11 (ii) an ASIO employee; or
12 (b) if the agency is the Australian Secret Intelligence Service:
13 (i) the Director-General of the Australian Secret
14 Intelligence Service; or
15 (ii) a staff member of the Australian Secret Intelligence
16 Service; or
17 (c) if the agency is the Australian Signals Directorate:
18 (i) the Director-General of the Australian Signals
19 Directorate; or
20 (ii) a staff member of the Australian Signals Directorate; or
21 (d) if the agency is an interception agency:
22 (i) the chief officer of the interception agency; or
23 (ii) an officer of the interception agency.

24 **Division 8—General provisions**

25 **317ZJ Immunity**

- 26 (1) A designated communications provider is not subject to any civil
27 liability for, or in relation to, an act or thing done by the provider:
28 (a) in compliance; or
29 (b) in good faith in purported compliance;
30 with:
31 (c) a technical assistance notice; or
32 (d) a technical capability notice.

- 1 (2) Paragraph (1)(b) does not apply to an act or thing done by a
2 designated communications provider unless the act or thing is in
3 connection with any or all of the eligible activities of the provider.
- 4 (3) An officer, employee or agent of a designated communications
5 provider is not subject to any civil liability for, or in relation to, an
6 act or thing done by the officer, employee or agent in connection
7 with an act or thing done by the provider:
8 (a) in compliance; or
9 (b) in good faith in purported compliance;
10 with:
11 (c) a technical assistance notice; or
12 (d) a technical capability notice.
- 13 (4) Paragraph (3)(b) does not apply to an act or thing done by a
14 designated communications provider unless the act or thing is in
15 connection with any or all of the eligible activities of the provider.

16 **317ZK Terms and conditions on which help is to be given etc.**

17 *Scope*

- 18 (1) This section applies if a designated communications provider is
19 subject to a requirement under:
20 (a) a technical assistance notice; or
21 (b) a technical capability notice;
22 unless:
23 (c) in the case of a requirement under a technical assistance
24 notice given by the Director-General of Security—the
25 Director-General of Security declares in writing that the
26 Director-General of Security is satisfied that it would be
27 contrary to the public interest for this section to apply to the
28 requirement; or
29 (d) in the case of a requirement under a technical assistance
30 notice given by the chief officer of an interception agency—
31 the chief officer declares in writing that the chief officer is
32 satisfied that it would be contrary to the public interest for
33 this section to apply to the requirement; or

- 1 (e) in the case of a requirement under a technical capability
2 notice—the Attorney-General declares in writing that the
3 Attorney-General is satisfied that it would be contrary to the
4 public interest for this section to apply to the requirement.
- 5 (2) In deciding whether it would be contrary to the public interest for
6 this section to apply to a requirement, the Director-General of
7 Security, the chief officer or the Attorney-General, as the case may
8 be, must have regard to the following matters:
- 9 (a) in the case of a requirement under a technical assistance
10 notice given by the chief officer of an interception agency or
11 a requirement under a technical capability notice that relates
12 to an interception agency—the interests of law enforcement;
- 13 (b) in the case of a requirement under a technical assistance
14 notice given by the Director-General of Security or a
15 requirement under a technical capability notice that relates to
16 ASIO—the interests of national security;
- 17 (c) the objects of this Act;
- 18 (d) the extent to which compliance with the requirement will
19 impose a regulatory burden on the provider;
- 20 (e) the reasons for the giving of the technical assistance notice or
21 technical capability notice, as the case requires;
- 22 (f) such other matters (if any) as the Director-General of
23 Security, the chief officer or the Attorney-General, as the
24 case may be, considers relevant.

25 *Basis of compliance*

- 26 (3) The designated communications provider must comply with the
27 requirement on the basis that the provider neither:
- 28 (a) profits from complying with the requirement; nor
29 (b) bears the reasonable costs of complying with the
30 requirement;
- 31 unless:
- 32 (c) the provider and the applicable costs negotiator otherwise
33 agree; or
34 (d) in the case of a requirement under a technical assistance
35 notice given by the Director-General of Security—the
36 Director-General of Security declares in writing that the

- 1 Director-General of Security is satisfied that it would be
2 contrary to the public interest for this subsection to apply to
3 the requirement; or
4 (e) in the case of a requirement under a technical assistance
5 notice given by the chief officer of an interception agency—
6 the chief officer declares in writing that the chief officer is
7 satisfied that it would be contrary to the public interest for
8 this subsection to apply to the requirement; or
9 (f) in the case of a requirement under a technical capability
10 notice—the Attorney-General declares in writing that the
11 Attorney-General is satisfied that it would be contrary to the
12 public interest for this subsection to apply to the requirement.

13 Note: For *applicable costs negotiator*, see subsection (16).

- 14 (3A) In deciding whether it would be contrary to the public interest for
15 subsection (3) to apply to the requirement, the Director-General of
16 Security, the chief officer or the Attorney-General, as the case may
17 be, must have regard to the following matters:
18 (a) in the case of a requirement under a technical assistance
19 notice given by the chief officer of an interception agency or
20 a requirement under a technical capability notice that relates
21 to an interception agency—the interests of law enforcement;
22 (b) in the case of a requirement under a technical assistance
23 notice given by the Director-General of Security or a
24 requirement under a technical capability notice that relates to
25 ASIO—the interests of national security;
26 (c) the objects of this Act;
27 (d) the extent to which compliance with the requirement will
28 impose a regulatory burden on the provider;
29 (e) the reasons for the giving of the technical assistance notice or
30 technical capability notice, as the case requires;
31 (f) such other matters (if any) as the Director-General of
32 Security, the chief officer or the Attorney-General, as the
33 case may be, considers relevant.

34 *Terms and conditions*

- 35 (4) The designated communications provider must comply with the
36 requirement on such terms and conditions as are:

Schedule 1 Industry assistance
Part 1 Amendments

- 1 (a) agreed between the following parties:
2 (i) the provider;
3 (ii) the applicable costs negotiator; or
4 (b) failing agreement, determined by an arbitrator appointed by
5 the parties.

6 Note: For *applicable costs negotiator*, see subsection (16).

- 7 (5) If:
8 (a) the parties fail to agree on the appointment of an arbitrator;
9 and
10 (b) one of the parties is a carrier or carriage service provider;
11 the ACMA is to appoint the arbitrator.

- 12 (6) If:
13 (a) the parties fail to agree on the appointment of an arbitrator;
14 and
15 (b) none of the parties is a carrier or carriage service provider;
16 the Attorney-General is to appoint the arbitrator.

- 17 (6A) Subsection (4) does not apply to the requirement if:
18 (a) in the case of a requirement under a technical assistance
19 notice given by the Director-General of Security—the
20 Director-General of Security declares in writing that the
21 Director-General of Security is satisfied that it would be
22 contrary to the public interest for subsection (4) to apply to
23 the requirement; or
24 (b) in the case of a requirement under a technical assistance
25 notice given by the chief officer of an interception agency—
26 the chief officer declares in writing that the chief officer is
27 satisfied that it would be contrary to the public interest for
28 subsection (4) to apply to the requirement; or
29 (c) in the case of a requirement under a technical capability
30 notice—the Attorney-General declares in writing that the
31 Attorney-General is satisfied that it would be contrary to the
32 public interest for subsection (4) to apply to the requirement.

- 33 (6B) In deciding whether it would be contrary to the public interest for
34 subsection (4) to apply to the requirement, the Director-General of

1 Security, the chief officer or the Attorney-General, as the case may
2 be, must have regard to the following matters:

- 3 (a) in the case of a requirement under a technical assistance
4 notice given by the chief officer of an interception agency or
5 a requirement under a technical capability notice that relates
6 to an interception agency—the interests of law enforcement;
7 (b) in the case of a requirement under a technical assistance
8 notice given by the Director-General of Security or a
9 requirement under a technical capability notice that relates to
10 ASIO—the interests of national security;
11 (c) the objects of this Act;
12 (d) the extent to which compliance with the requirement will
13 impose a regulatory burden on the provider;
14 (e) the reasons for the giving of the technical assistance notice or
15 technical capability notice, as the case requires;
16 (f) such other matters (if any) as the Director-General of
17 Security, the chief officer or the Attorney-General, as the
18 case may be, considers relevant.

19 *Arbitration*

- 20 (7) An arbitrator appointed under subsection (5) or (6) must be:
21 (a) a person specified under subsection (8); or
22 (b) a person who belongs to a class of persons specified under
23 subsection (11).
24 (8) The Home Affairs Minister may, by writing, specify one or more
25 persons for the purposes of paragraph (7)(a).
26 (9) An instrument made under subsection (8) is not a legislative
27 instrument.
28 (10) Subsection 33(3AB) of the *Acts Interpretation Act 1901* does not
29 apply to the power conferred by subsection (8).
30 (11) The Home Affairs Minister may, by legislative instrument, specify
31 a class of persons for the purposes of paragraph (7)(b).
32 (12) Before making an instrument under subsection (8) or (11), the
33 Home Affairs Minister must consult the Attorney-General.

1 (13) If an arbitration under this section is conducted by an arbitrator
2 appointed by the ACMA, the cost of the arbitration must be
3 apportioned equally between the parties.

4 (14) The Home Affairs Minister may, by legislative instrument, make
5 provision for and in relation to the conduct of an arbitration under
6 this section.

7 *Acquisition of property*

8 (15) This section has no effect to the extent (if any) to which its
9 operation would result in an acquisition of property (within the
10 meaning of paragraph 51(xxxi) of the Constitution) otherwise than
11 on just terms (within the meaning of that paragraph).

12 *Applicable costs negotiator*

13 (16) For the purposes of this section, the *applicable costs negotiator* is:
14 (a) in the case of a requirement under a technical assistance
15 notice given by the Director-General of Security—the
16 Director-General of Security; or
17 (b) in the case of a requirement under a technical assistance
18 notice given by the chief officer of an interception agency—
19 the chief officer; or
20 (c) in the case of a requirement under a technical capability
21 notice—the person specified in the notice, in accordance with
22 subsection 317T(12), as the applicable costs negotiator for
23 the notice.

24 *Technical capability notice that relates to ASIO*

25 (17) For the purposes of this section, a technical capability notice
26 relates to ASIO if the acts or things specified in the notice:
27 (a) are directed towards ensuring that a designated
28 communications provider is capable of giving listed help
29 (within the meaning of section 317T) to ASIO in relation to a
30 matter covered by paragraph 317T(2)(a); or
31 (b) are by way of giving help to ASIO in relation to a matter
32 covered by paragraph 317T(2)(b).

1 *Technical capability notice that relates to an interception agency*

- 2 (18) For the purposes of this section, a technical capability notice
3 relates to an interception agency if the acts or things specified in
4 the notice:
5 (a) are directed towards ensuring that a designated
6 communications provider is capable of giving listed help
7 (within the meaning of section 317T) to the interception
8 agency in relation to a matter covered by
9 paragraph 317T(2)(a); or
10 (b) are by way of giving help to the interception agency in
11 relation to a matter covered by paragraph 317T(2)(b).

12 *Technical assistance notice information*

- 13 (19) For the purposes of this Part, information about a declaration
14 under:
15 (a) paragraph (1)(c); or
16 (b) paragraph (1)(d); or
17 (c) paragraph (3)(d); or
18 (d) paragraph (3)(e); or
19 (e) paragraph (6A)(a); or
20 (f) paragraph (6A)(b);
21 is taken to be information about a technical assistance notice.

22 *Technical capability notice information*

- 23 (20) For the purposes of this Part, information about a declaration under
24 paragraph (1)(e), (3)(f) or (6A)(c) is taken to be information about
25 a technical capability notice.

26 **317ZKA Notification obligations**

- 27 (1) If the Director-General of Security makes a declaration under
28 paragraph 317ZK(1)(c), (3)(d) or (6A)(a), the Director-General of
29 Security must, within 7 days after making the declaration, notify
30 the Inspector-General of Intelligence and Security of the making of
31 the declaration.

- 1 (2) If the chief officer of an interception agency makes a declaration
2 under paragraph 317ZK(1)(d), (3)(e) or (6A)(b), the chief officer
3 must, within 7 days after making the declaration, notify the
4 Commonwealth Ombudsman of the making of the declaration.
- 5 (3) If:
- 6 (a) the Attorney-General makes a declaration under
7 paragraph 317ZK(1)(e), (3)(f) or (6A)(c) in relation to a
8 technical capability notice; and
- 9 (b) the acts or things specified in the notice:
- 10 (i) are directed towards ensuring that a designated
11 communications provider is capable of giving listed
12 help (within the meaning of section 317T) to ASIO in
13 relation to a matter covered by paragraph 317T(2)(a); or
- 14 (ii) are by way of giving help to ASIO in relation to a
15 matter covered by paragraph 317T(2)(b);
- 16 the Attorney-General must, within 7 days after making the
17 declaration, notify the Inspector-General of Intelligence and
18 Security of the making of the declaration.
- 19 (4) If:
- 20 (a) the Attorney-General makes a declaration under
21 paragraph 317K(1)(e), (3)(f) or (6A)(c) in relation to a
22 technical capability notice; and
- 23 (b) the acts or things specified in the notice:
- 24 (i) are directed towards ensuring that a designated
25 communications provider is capable of giving listed
26 help (within the meaning of section 317T) to an
27 interception agency in relation to a matter covered by
28 paragraph 317T(2)(a); or
- 29 (ii) are by way of giving help to an interception agency in
30 relation to a matter covered by paragraph 317T(2)(b);
- 31 the Attorney-General must, within 7 days after making the
32 declaration, notify the Commonwealth Ombudsman of the making
33 of the declaration.
- 34 (5) A failure to comply with subsection (1), (2), (3) or (4) does not
35 affect the validity of a declaration under:
- 36 (a) paragraph 317ZK(1)(c); or

- 1 (b) paragraph 317ZK(1)(d); or
- 2 (c) paragraph 317ZK(1)(e); or
- 3 (d) paragraph 317ZK(3)(d); or
- 4 (e) paragraph 317ZK(3)(e); or
- 5 (f) paragraph 317ZK(3)(f); or
- 6 (g) paragraph 317ZK(6A)(a); or
- 7 (h) paragraph 317ZK(6A)(b); or
- 8 (i) paragraph 317ZK(6A)(c).

9 **317ZL Service of notices etc.**

10 *Scope*

- 11 (1) This section applies to:
- 12 (a) a summons or process in any proceedings under, or
 - 13 connected with, this Part; or
 - 14 (b) a summons or process in any proceedings under, or
 - 15 connected with, the *Regulatory Powers (Standard*
 - 16 *Provisions) Act 2014*, so far as that Act relates to this Part; or
 - 17 (c) a technical assistance notice or any other notice under this
 - 18 Part; or
 - 19 (d) a notice under the *Regulatory Powers (Standard Provisions)*
 - 20 *Act 2014*, so far as that Act relates to this Part; or
 - 21 (e) a technical capability notice.

22 *Address for service of summons, process or notice*

- 23 (2) If:
- 24 (a) the summons, process or notice, as the case may be, is
 - 25 required to be served on, or given to, a designated
 - 26 communications provider; and
 - 27 (b) the designated communications provider has nominated an
 - 28 address for service in a document given by the provider to:
 - 29 (i) the Attorney-General; or
 - 30 (ii) the Communications Access Co-ordinator; or
 - 31 (iii) the Director-General of Security; or
 - 32 (iv) the chief officer of an interception agency;

1 the summons, process, or notice, as the case may be, is taken to
2 have been served on, or given to, the provider if it is left at, or sent
3 by pre-paid post to, the nominated address for service.

4 (3) If:

- 5 (a) the summons, process or notice, as the case may be, is
6 required to be served on, or given to, a designated
7 communications provider; and
8 (b) the designated communications provider has nominated an
9 electronic address for service in a document given by the
10 provider to:
11 (i) the Attorney-General; or
12 (ii) the Communications Access Co-ordinator; or
13 (iii) the Director-General of Security; or
14 (iv) the chief officer of an interception agency;
15 the summons, process or notice, as the case may be, is taken to
16 have been served on, or given to, the provider if it is sent to the
17 nominated electronic address for service.

18 *Service of summons, process or notice on agent etc.*

19 (4) If:

- 20 (a) the summons, process or notice, as the case may be, is
21 required to be served on, or given to, a body corporate
22 incorporated outside Australia; and
23 (b) the body corporate does not have a registered office or a
24 principal office in Australia; and
25 (c) the body corporate has an agent in Australia;
26 the summons, process or notice, as the case may be, is taken to
27 have been served on, or given to, the body corporate if it is served
28 on, or given to, the agent.

29 (5) If:

- 30 (a) the summons, process or notice, as the case may be, is
31 required to be served on, or given to, a body corporate
32 incorporated outside Australia; and
33 (b) the body corporate does not have a registered office or a
34 principal office in Australia; and

1 (c) the body corporate carries on business, or conducts activities,
2 at an address in Australia;
3 the summons, process or notice, as the case may be, is taken to
4 have been served on, or given to, the body corporate if it is left at,
5 or sent by pre-paid post to, that address.

6 *Other matters*

- 7 (6) Subsections (2), (3), (4) and (5) have effect in addition to:
8 (a) section 28A of the *Acts Interpretation Act 1901*; and
9 (b) sections 587 and 588 of this Act.

10 Note: Section 28A of the *Acts Interpretation Act 1901* deals with the service
11 of documents.

12 **317ZM Interception agency—chief officer and officer**

13 For the purposes of this Part, the following table defines:

- 14 (a) **chief officer** of an interception agency; and
15 (b) **officer** of an interception agency.

16

Chief officer and officers of interception agencies			
Item	Column 1	Column 2	Column 3
	Interception agency	Chief officer	Officer
1	Australian Federal Police	the Commissioner (within the meaning of the <i>Australian Federal Police Act 1979</i>)	a member or special member of the Australian Federal Police
3	Australian Crime Commission	Chief Executive Officer of the Australian Crime Commission	(a) the Chief Executive Officer of the Australian Crime Commission; or (b) an examiner (within the meaning of the <i>Australian Crime Commission Act 2002</i>); or (c) a member of the staff of the ACC (within the meaning

Schedule 1 Industry assistance
Part 1 Amendments

Chief officer and officers of interception agencies			
Item	Column 1	Column 2	Column 3
	Interception agency	Chief officer	Officer
			of the <i>Australian Crime Commission Act 2002</i>)
4	Police Force of a State or the Northern Territory	the Commissioner of Police (however designated) of that State or Territory	an officer of that Police Force

1 **317ZN Delegation by Director-General of Security**

- 2 (1) The Director-General of Security may, by writing, delegate any or
3 all of the functions or powers of the Director-General of Security
4 under Division 2, 3 or 6 to a senior position-holder (within the
5 meaning of the *Australian Security Intelligence Organisation Act*
6 *1979*).
- 7 (2) A delegate must comply with any written directions of the
8 Director-General of Security.

9 **317ZP Delegation by Director-General of the Australian Secret**
10 **Intelligence Service**

- 11 (1) The Director-General of the Australian Secret Intelligence Service
12 may, by writing, delegate any or all of the functions or powers of
13 the Director-General of the Australian Secret Intelligence Service
14 under Division 2 or 6 to a person who:
15 (a) is a staff member of the Australian Secret Intelligence
16 Service; and
17 (b) holds, or is acting in, a position in the Australian Secret
18 Intelligence Service that is equivalent to, or higher than, a
19 position occupied by an SES employee.
- 20 (2) A delegate must comply with any written directions of the
21 Director-General of the Australian Secret Intelligence Service.

1 **317ZQ Delegation by Director-General of the Australian Signals**
2 **Directorate**

3 (1) The Director-General of the Australian Signals Directorate may, by
4 writing, delegate any or all of the functions or powers of the
5 Director-General of the Australian Signals Directorate under
6 Division 2 or 6 to a person:

7 (a) who is a staff member of the Australian Signals Directorate;
8 and

9 (b) who:

10 (i) is an SES employee, or acting SES employee, in the
11 Australian Signals Directorate; or

12 (ii) holds, or is acting in, a position in the Australian Signals
13 Directorate that is equivalent to, or higher than, a
14 position occupied by an SES employee.

15 (2) A delegate must comply with any written directions of the
16 Director-General of the Australian Signals Directorate.

17 **317ZR Delegation by the chief officer of an interception agency**

18 (1) The chief officer of an interception agency mentioned in an item of
19 column 1 of the following table may, by writing, delegate any or
20 all of the functions or powers of the chief officer under Division 2,
21 3 or 6 to a person mentioned in column 2 of the item.
22

Potential delegates

Item	Column 1	Column 2
	Interception agency	Potential delegates
1	Australian Federal Police	(a) a Deputy Commissioner (within the meaning of the <i>Australian Federal Police Act 1979</i>); or (b) a senior executive AFP employee (within the meaning of the <i>Australian Federal Police Act 1979</i>)
3	Australian Crime Commission	a member of the staff of the ACC (within the meaning of the <i>Australian Crime Commission Act 2002</i>) who is an SES employee or acting SES employee
4	Police Force of a State or the	(a) an Assistant Commissioner of the Police Force or a person holding equivalent rank; or

Schedule 1 Industry assistance
Part 1 Amendments

Potential delegates

Item	Column 1	Column 2
	Interception agency	Potential delegates
	Northern Territory	(b) a Superintendent of the Police Force or a person holding equivalent rank

1 (2) A delegate must comply with any written directions of the chief
2 officer.

3 *Executive level*

4 (3) For the purposes of this section, a person is at *executive level*, in
5 relation to an interception agency of New South Wales, if the
6 person occupies an office or position at an equivalent level to that
7 of a Public Service senior executive (within the meaning of the
8 *Government Sector Employment Act 2013* (NSW)).

9 (4) For the purposes of this section, a person is at *executive level*, in
10 relation to an interception agency of Victoria, if the person
11 occupies an office or position at an equivalent level to that of an
12 executive (within the meaning of the *Public Administration Act*
13 *2004* (Vic.)).

14 (5) For the purposes of this section, a person is at *executive level*, in
15 relation to an interception agency of South Australia, if the person
16 occupies an office or position at an equivalent level to that of an
17 executive employee (within the meaning of the *Public Sector Act*
18 *2009* (SA)).

19 **317ZRA Relationship of this Part to parliamentary privileges and**
20 **immunities**

21 To avoid doubt, this Part does not affect the law relating to the
22 powers, privileges and immunities of any of the following:

- 23 (a) each House of the Parliament;
24 (b) the members of each House of the Parliament;
25 (c) the committees of each House of the Parliament and joint
26 committees of both Houses of the Parliament.

1 **317ZRB Inspection of records**

- 2 (1) An Ombudsman official may inspect the records of an interception
3 agency to determine the extent of compliance with this Part by:
4 (a) the agency; and
5 (b) the chief officer of the agency; and
6 (c) officers of the agency.
- 7 (2) The chief officer of an interception agency must ensure that
8 officers of the agency give an Ombudsman official any assistance
9 the Ombudsman official reasonably requires to enable the
10 Ombudsman official to exercise the power conferred by
11 subsection (1).

12 *Report*

- 13 (3) The Commonwealth Ombudsman may make a written report to the
14 Home Affairs Minister on the results of one or more inspections
15 under subsection (1).
- 16 (4) A report under subsection (3) must not include information which,
17 if made public, could reasonably be expected to:
18 (a) prejudice an investigation or prosecution; or
19 (b) compromise any interception agency's operational activities
20 or methodologies.
- 21 (5) If:
22 (a) the Commonwealth Ombudsman makes a report under
23 subsection (3); and
24 (b) the report relates to an inspection under subsection (1) of the
25 records of an interception agency of a State or Territory;
26 the Commonwealth Ombudsman must give a copy of the report to
27 the chief officer of the interception agency.
- 28 (6) If the Home Affairs Minister receives a report under
29 subsection (3), the Home Affairs Minister must cause a copy of the
30 report to be tabled in each House of the Parliament within 15
31 sitting days of that House after the Home Affairs Minister receives
32 the report.

- 1 (7) Before tabling the copy of the report, the Home Affairs Minister
2 may delete from the copy information that, if made public, could
3 reasonably be expected to:
4 (a) prejudice an investigation or prosecution; or
5 (b) compromise any interception agency's operational activities
6 or methodologies.

7 **317ZS Annual reports**

- 8 (1) The Home Affairs Minister must, as soon as practicable after each
9 30 June, cause to be prepared a written report that sets out:
10 (a) the number of technical assistance requests that were given
11 during the year ending on that 30 June by the chief officers of
12 interception agencies; and
13 (b) the number of technical assistance notices that were given
14 during the year ending on that 30 June by the chief officers of
15 interception agencies; and
16 (c) the number of technical capability notices that were:
17 (i) given during the year ending on that 30 June; and
18 (ii) directed towards ensuring that designated
19 communications providers are capable of giving help to
20 interception agencies; and
21 (d) if any technical assistance requests, technical assistance
22 notices or technical capability notices given during the year
23 ending on that 30 June related to the enforcement of the
24 criminal law so far as it relates to one or more kinds of
25 serious Australian offences—those kinds of serious
26 Australian offences.
- 27 (2) A report under subsection (1) must be included in the report
28 prepared under subsection 186(2) of the *Telecommunications*
29 *(Interception and Access) Act 1979* relating to the year ending on
30 that 30 June.

31 **317ZT Alternative constitutional basis**

- 32 (1) Without limiting its effect apart from this section, this Part also has
33 effect as provided by this section.

1 (2) This Part also has the effect it would have if each reference in this
2 Part to a designated communications provider were, by express
3 provision, confined to a designated communications provider that
4 is a constitutional corporation.

5 **7A After paragraph 570(3)(a)**

6 Insert:

7 (aa) in the case of a contravention of subsection 317ZA(1) or
8 (2)—47,619 penalty units for each contravention; or

9 **7B After subsection 570(4B)**

10 Insert:

11 (4C) Subsection (4) does not apply to a contravention of
12 subsection 317ZA(1) or (2).

13 (4D) The pecuniary penalty payable under subsection (1) by a person
14 other than a body corporate for a contravention of
15 subsection 317ZA(1) or (2) is not to exceed 238 penalty units for
16 each contravention.

17 ***Telecommunications (Interception and Access) Act 1979***

18 **7C At the end of section 83**

19 Add:

20 (4) If:

21 (a) the performance of a function, or the exercise of a power,
22 conferred by Part 15 of the *Telecommunications Act 1997* is
23 in connection with an interception warrant; and

24 (b) a Commonwealth agency has records that relate to the
25 performance of that function or the exercise of that power;
26 the Ombudsman may inspect those records in order to ascertain the
27 extent to which the agency's officers have complied with Part 15
28 of the *Telecommunications Act 1997*.

29 **7D Subsection 84(1)**

30 Omit “and (3)”, substitute “, (3) and (4)”.

1 **7E After subsection 186B(1)**

2 Insert:

3 (1A) If:

4 (a) the performance of a function, or the exercise of a power,
5 conferred by Part 15 of the *Telecommunications Act 1997* is
6 in connection with:

7 (i) a stored communications warrant; or

8 (ii) an authorisation under Division 3, 4 or 4A of Part 4-1;
9 and

10 (b) an enforcement agency has records that relate to the
11 performance of that function or the exercise of that power;
12 the Ombudsman may inspect those records in order to determine
13 the extent of compliance with Part 15 of the *Telecommunications*
14 *Act 1997* by the agency and its officers.

15 **7F Section 187N (heading)**

16 Omit “Part”, substitute “**this Part and the amendments made by the**
17 ***Telecommunications and Other Legislation Amendment (Assistance***
18 ***and Access) Act 2018*”.**

19 **7G Subsection 187N(1)**

20 After “this Part”, insert “and the amendments made by the
21 *Telecommunications and Other Legislation Amendment (Assistance and*
22 *Access) Act 2018*”.

1 **Part 2—Amendments contingent on the**
2 **commencement of the Federal Circuit and**
3 **Family Court of Australia Act 2018**

4 *Telecommunications Act 1997*

5 **8 Subsections 317ZC(3), 317ZD(3) and 317ZE(3)**

6 Omit “Federal Circuit Court of Australia”, substitute “Federal Circuit
7 and Family Court of Australia (Division 2)”.

1 **Schedule 2—Computer access warrants etc.**

2 **Part 1—Amendments**

3 *Australian Security Intelligence Organisation Act 1979*

4 **1 Section 4**

5 Insert:

6 *intercept a communication passing over a telecommunications*
7 *system* has the same meaning as in the *Telecommunications*
8 *(Interception and Access) Act 1979*.

9 **2 Subsection 24(4) (definition of *relevant device recovery***
10 ***provision*)**

11 After “subsection”, insert “25A(8),”.

12 **3 Subsection 24(4) (definition of *relevant device recovery***
13 ***provision*)**

14 Omit “or (3B)”, substitute “, (3B) or (3C), 27E(6)”.

15 **4 Paragraph 25A(4)(ab)**

16 Repeal the paragraph, substitute:

17 (ab) if, having regard to other methods (if any) of obtaining access
18 to the relevant data which are likely to be as effective, it is
19 reasonable in all the circumstances to do so:

20 (i) using any other computer or a communication in transit
21 to access the relevant data; and

22 (ii) if necessary to achieve that purpose—adding, copying,
23 deleting or altering other data in the computer or the
24 communication in transit;

25 **5 After paragraph 25A(4)(ab)**

26 Insert:

27 (ac) removing a computer or other thing from premises for the
28 purposes of doing any thing specified in the warrant in

1 accordance with this subsection, and returning the computer
2 or other thing to the premises;

3 **6 After paragraph 25A(4)(b)**

4 Insert:

5 (ba) intercepting a communication passing over a
6 telecommunications system, if the interception is for the
7 purposes of doing any thing specified in the warrant in
8 accordance with this subsection;

9 **6A After subsection 25A(4)**

10 Insert:

11 (4A) If:

- 12 (a) the warrant authorises the removal of a computer or other
13 thing from premises as mentioned in paragraph (4)(ac); and
14 (b) a computer or thing is removed from the premises in
15 accordance with the warrant;
16 the computer or thing must be returned to the premises:
17 (c) if returning the computer or thing would be prejudicial to
18 security—when returning the computer or thing would no
19 longer be prejudicial to security; or
20 (d) otherwise—within a reasonable period.

21 **7 At the end of section 25A**

22 Add:

23 *Concealment of access etc.*

- 24 (8) If any thing has been done in relation to a computer under:
25 (a) the warrant; or
26 (b) this subsection;
27 the Organisation is authorised to do any of the following:
28 (c) any thing reasonably necessary to conceal the fact that any
29 thing has been done under the warrant or under this
30 subsection;
31 (d) enter any premises where the computer is reasonably
32 believed to be, for the purposes of doing the things
33 mentioned in paragraph (c);
-

- 1 (e) enter any other premises for the purposes of gaining entry to
2 or exiting the premises referred to in paragraph (d);
- 3 (f) remove the computer or another thing from any place where
4 it is situated for the purposes of doing the things mentioned
5 in paragraph (c), and returning the computer or other thing to
6 that place;
- 7 (g) if, having regard to other methods (if any) of doing the things
8 mentioned in paragraph (c) which are likely to be as
9 effective, it is reasonable in all the circumstances to do so:
- 10 (i) use any other computer or a communication in transit to
11 do those things; and
- 12 (ii) if necessary to achieve that purpose—add, copy, delete
13 or alter other data in the computer or the communication
14 in transit;
- 15 (h) intercept a communication passing over a
16 telecommunications system, if the interception is for the
17 purposes of doing any thing mentioned in this subsection;
- 18 (i) any other thing reasonably incidental to any of the above;
- 19 at the following time:
- 20 (j) at any time while the warrant is in force or within 28 days
21 after it ceases to be in force;
- 22 (k) if none of the things mentioned in paragraph (c) are done
23 within the 28-day period mentioned in paragraph (j)—at the
24 earliest time after that 28-day period at which it is reasonably
25 practicable to do the things mentioned in paragraph (c).
- 26 (9) Subsection (8) does not authorise the doing of a thing that is likely
27 to:
- 28 (a) materially interfere with, interrupt or obstruct:
- 29 (i) a communication in transit; or
- 30 (ii) the lawful use by other persons of a computer;
- 31 unless the doing of the thing is necessary to do one or more
32 of the things specified in subsection (8); or
- 33 (b) cause any other material loss or damage to other persons
34 lawfully using a computer.
- 35 (10) If a computer or another thing is removed from a place in
36 accordance with paragraph (8)(f), the computer or thing must be
37 returned to that place:
-

- 1 (a) if returning the computer or thing would be prejudicial to
2 security—when returning the computer or thing would no
3 longer be prejudicial to security; or
4 (b) otherwise—within a reasonable period.

5 **8 After subsection 27A(3B)**

6 Insert:

7 (3C) If any thing has been done in relation to a computer under:

- 8 (a) a warrant under this section that authorises the Organisation
9 to do acts or things referred to in subsection 25A(4); or
10 (b) this subsection;

11 the Organisation is authorised to do any of the following:

- 12 (c) any thing reasonably necessary to conceal the fact that any
13 thing has been done under the warrant or under this
14 subsection;
15 (d) enter any premises where the computer is reasonably
16 believed to be, for the purposes of doing the things
17 mentioned in paragraph (c);
18 (e) enter any other premises for the purposes of gaining entry to
19 or exiting the premises referred to in paragraph (d);
20 (f) remove the computer or another thing from any place where
21 it is situated for the purposes of doing the things mentioned
22 in paragraph (c), and returning the computer or other thing to
23 that place;
24 (g) if, having regard to other methods (if any) of doing the things
25 mentioned in paragraph (c) which are likely to be as
26 effective, it is reasonable in all the circumstances to do so:
27 (i) use any other computer or a communication in transit to
28 do those things; and
29 (ii) if necessary to achieve that purpose—add, copy, delete
30 or alter other data in the computer or the communication
31 in transit;
32 (h) intercept a communication passing over a
33 telecommunications system, if the interception is for the
34 purposes of doing any thing mentioned in this subsection;
35 (i) any other thing reasonably incidental to any of the above;

36 at the following time:

- 1 (j) at any time while the warrant is in force or within 28 days
2 after it ceases to be in force;
- 3 (k) if none of the things mentioned in paragraph (c) are done
4 within the 28-day period mentioned in paragraph (j)—at the
5 earliest time after that 28-day period at which it is reasonably
6 practicable to do the things mentioned in paragraph (c).
- 7 (3D) Subsection (3C) does not authorise the doing of a thing that is
8 likely to:
- 9 (a) materially interfere with, interrupt or obstruct:
- 10 (i) a communication in transit; or
11 (ii) the lawful use by other persons of a computer;
12 unless the doing of the thing is necessary to do one or more
13 of the things specified in subsection (3C); or
- 14 (b) cause any other material loss or damage to other persons
15 lawfully using a computer.
- 16 (3E) If a computer or another thing is removed from a place in
17 accordance with paragraph (3C)(f), the computer or thing must be
18 returned to that place:
- 19 (a) if returning the computer or thing would be prejudicial to
20 security—when returning the computer or thing would no
21 longer be prejudicial to security; or
22 (b) otherwise—within a reasonable period.

23 9 Paragraph 27E(2)(d)

24 Repeal the paragraph, substitute:

- 25 (d) if, having regard to other methods (if any) of obtaining access
26 to the relevant data which are likely to be as effective, it is
27 reasonable in all the circumstances to do so:
- 28 (i) use any other computer or a communication in transit
29 for the purpose referred to in paragraph (c); and
30 (ii) if necessary to achieve that purpose—add, copy, delete
31 or alter other data in the computer or the communication
32 in transit;

33 10 After paragraph 27E(2)(d)

34 Insert:

- 1 (da) remove a computer or other thing from premises for the
2 purposes of doing any thing authorised under this subsection,
3 and returning the computer or other thing to the premises;

4 **11 After paragraph 27E(2)(e)**

5 Insert:

- 6 (ea) intercept a communication passing over a
7 telecommunications system, if the interception is for the
8 purposes of doing any thing authorised under this subsection;

9 **11A After subsection 27E(3)**

10 Insert:

11 *Return of computer or other thing*

12 (3A) If:

13 (a) an authorisation under subsection (2) authorises the removal
14 of a computer or other thing from premises as mentioned in
15 paragraph (2)(da); and

16 (b) a computer or thing is removed from the premises in
17 accordance with the authorisation;

18 the computer or thing must be returned to the premises:

19 (c) if returning the computer or thing would be prejudicial to
20 security—when returning the computer or thing would no
21 longer be prejudicial to security; or

22 (d) otherwise—within a reasonable period.

23 **12 At the end of section 27E**

24 Add:

25 *Concealment of access etc.*

26 (6) If any thing has been done in relation to a computer under:

27 (a) a subsection (2) authorisation; or

28 (b) under this subsection;

29 the Organisation is authorised to do any of the following:

30 (c) any thing reasonably necessary to conceal the fact that any
31 thing has been done under the subsection (2) authorisation or
32 under this subsection;

- 1 (d) enter any premises where the computer is reasonably
2 believed to be, for the purposes of doing the things
3 mentioned in paragraph (c);
- 4 (e) enter any other premises for the purposes of gaining entry to
5 or exiting the premises referred to in paragraph (d);
- 6 (f) remove the computer or another thing from any place where
7 it is situated for the purposes of doing the things mentioned
8 in paragraph (c), and returning the computer or other thing to
9 that place;
- 10 (g) if, having regard to other methods (if any) of doing the things
11 mentioned in paragraph (c) which are likely to be as
12 effective, it is reasonable in all the circumstances to do so:
- 13 (i) use any other computer or a communication in transit to
14 do those things; and
- 15 (ii) if necessary to achieve that purpose—add, copy, delete
16 or alter other data in the computer or the communication
17 in transit;
- 18 (h) intercept a communication passing over a
19 telecommunications system, if the interception is for the
20 purposes of doing any thing mentioned in this subsection;
- 21 (i) any other thing reasonably incidental to any of the above;
- 22 at the following time:
- 23 (j) at any time while the authorisation is in force or within 28
24 days after it ceases to be in force;
- 25 (k) if none of the things mentioned in paragraph (c) are done
26 within the 28-day period mentioned in paragraph (j)—at the
27 earliest time after that 28-day period at which it is reasonably
28 practicable to do the things mentioned in paragraph (c).
- 29 (7) Subsection (6) does not authorise the doing of a thing that is likely
30 to:
- 31 (a) materially interfere with, interrupt or obstruct:
- 32 (i) a communication in transit; or
- 33 (ii) the lawful use by other persons of a computer;
- 34 unless the doing of the thing is necessary to do one or more
35 of the things specified in subsection (6); or
- 36 (b) cause any other material loss or damage to other persons
37 lawfully using a computer.
-

- 1 (8) If a computer or another thing is removed from a place in
2 accordance with paragraph (6)(f), the computer or thing must be
3 returned to the place:
4 (a) if returning the computer or thing would be prejudicial to
5 security—when returning the computer or thing would no
6 longer be prejudicial to security; or
7 (b) otherwise—within a reasonable period.

8 **13 Subsection 33(1)**

9 Repeal the subsection.

10 **13A Section 34 (at the end of the heading)**

11 Add “—general”.

12 **14 Paragraph 34(2)(b)**

13 After “25A(4)”, insert “or (8) or 27A(3C)”.

14 **15 Paragraph 34(2)(b)**

15 After “27E(2)”, insert “or (6)”.

16 **16 At the end of section 34**

17 Add:

- 18 (3) For the purposes of this section, any thing done under
19 subsection 25A(8) is taken to have been done under a warrant
20 issued under section 25A.
21 (4) For the purposes of this section, any thing done under
22 subsection 27A(3C) is taken to have been done under a warrant
23 issued under section 27A.
24 (5) For the purposes of this section, any thing done under
25 subsection 27E(6) is taken to have been done under a warrant
26 issued under section 27C.

27 **16A After section 34**

28 Insert:

1 **34A Director-General to report to Attorney-General—concealment**
2 **of access**

3 (1) If:

- 4 (a) a warrant issued under this Division has ceased to be in force;
5 and
6 (b) during a prescribed post-cessation period of the warrant, a
7 thing was done under subsection 25A(8), 27A(3C) or 27E(6)
8 in connection with the warrant; and
9 (c) the thing has not been dealt with in a report under
10 subsection 34(1);

11 the Director-General must:

- 12 (d) give the Attorney-General a written report on the extent to
13 which doing the thing has assisted the Organisation in
14 carrying out its functions; and
15 (e) do so as soon as practicable after the end of that period.

16 (2) If:

- 17 (a) a warrant issued under this Division has ceased to be in force;
18 and
19 (b) as at the end of a prescribed post-cessation period of the
20 warrant, it is likely that a thing will be done under
21 subsection 25A(8), 27A(3C) or 27E(6) in connection with the
22 warrant;

23 the Director-General must:

- 24 (c) give the Attorney-General a written report on the extent to
25 which doing the thing will assist the Organisation in carrying
26 out its functions; and
27 (d) do so as soon as practicable after the end of that period.

28 *Prescribed post-cessation period*

29 (3) For the purposes of this section, each of the following periods is a
30 ***prescribed post-cessation period*** of a warrant:

- 31 (a) the 3-month period beginning immediately after the warrant
32 ceased to be in force;
33 (b) each subsequent 3-month period.

1 **17 Subsection 34AA(5) (definition of *relevant authorising***
2 ***provision*)**

3 Before “26B(5)”, insert “25A(8)”.

4 **18 Subsection 34AA(5) (definition of *relevant authorising***
5 ***provision*)**

6 Omit “or (3B)”, substitute “, (3B) or (3C), 27E(6)”.

7 ***Mutual Assistance in Criminal Matters Act 1987***

8 **25 Subsection 3(1) (definition of *protected information*)**

9 After “44(1)(a)”, insert “(aa)”.

10 **26 After Part IIIA**

11 Insert:

12 **Part IIIBB—Assistance in relation to data held in**
13 **computers**
14

15 **15CB Simplified outline of this Part**

- 16
- 17
- 18
- 19
- 20
- 21
- 22
- 23
- If a foreign country requests the Attorney-General to arrange for access to data held in a computer, the Attorney-General may authorise an eligible law enforcement officer to apply for a computer access warrant under section 27A of the *Surveillance Devices Act 2004*.
 - The authorisation relates to an investigation, or investigative proceeding, relating to a criminal matter involving an offence against the law of the foreign country.

24 Note: See subsection 27A(4) of the *Surveillance Devices Act 2004*.

1 **15CC Requests by foreign countries for assistance in relation to data**
2 **held in computers**

3 (1) The Attorney-General may, in the Attorney-General's discretion,
4 authorise an eligible law enforcement officer, in writing, to apply
5 for a computer access warrant under section 27A of the
6 *Surveillance Devices Act 2004* if the Attorney-General is satisfied
7 that:

8 (a) an investigation, or investigative proceeding, relating to a
9 criminal matter involving an offence against the law of a
10 foreign country (the **requesting country**) that is punishable
11 by a maximum penalty of imprisonment for 3 years or more,
12 imprisonment for life or the death penalty has commenced in
13 the requesting country; and

14 (b) the requesting country requests the Attorney-General to
15 arrange for access to data held in a computer (the **target**
16 **computer**); and

17 (c) the requesting country has given appropriate undertakings in
18 relation to:

19 (i) ensuring that data obtained as a result of access under
20 the warrant will only be used for the purpose for which
21 it is communicated to the requesting country; and

22 (ii) the destruction of a document or other thing containing
23 data obtained as a result of access under the warrant;
24 and

25 (iii) any other matter the Attorney-General considers
26 appropriate.

27 (2) The target computer may be any one or more of the following:

28 (a) a particular computer;

29 (b) a computer on particular premises;

30 (c) a computer associated with, used by or likely to be used by, a
31 person (whose identity may or may not be known).

32 (3) In this section:

33 **computer** has the same meaning as in the *Surveillance Devices Act*
34 *2004*.

1 **data** has the same meaning as in the *Surveillance Devices Act*
2 *2004*.

3 **data held in a computer** has the same meaning as in the
4 *Surveillance Devices Act 2004*.

5 **eligible law enforcement officer** means a person mentioned in
6 column 3 of item 5 of the table in subsection 6A(6), or in column 3
7 of item 5 of the table in subsection 6A(7), of the *Surveillance*
8 *Devices Act 2004*.

9 *Surveillance Devices Act 2004*

10 **27 Title**

11 After “**devices**”, insert “**and access to data held in computers**”.

12 **28 After paragraph 3(a)**

13 Insert:

- 14 (aaa) to establish procedures for law enforcement officers to obtain
15 warrants and emergency authorisations that:
16 (i) are for access to data held in computers; and
17 (ii) relate to criminal investigations and the location and
18 safe recovery of children to whom recovery orders
19 relate; and

20 **29 After paragraph 3(aa)**

21 Insert:

- 22 (aaaa) to establish procedures for law enforcement officers to obtain
23 warrants for access to data held in computers in cases where
24 a control order is in force, and access to the data would be
25 likely to substantially assist in:
26 (i) protecting the public from a terrorist act; or
27 (ii) preventing the provision of support for, or the
28 facilitation of, a terrorist act; or
29 (iii) preventing the provision of support for, or the
30 facilitation of, the engagement in a hostile activity in a
31 foreign country; or

- 1 (iv) determining whether the control order, or any
2 succeeding control order, has been, or is being,
3 complied with; and

4 **30 After paragraph 3(b)**

5 Insert:

- 6 (ba) to restrict the use, communication and publication of
7 information that is obtained through accessing data held in
8 computers or that is otherwise connected with computer data
9 access operations; and

10 **31 Paragraph 3(c)**

11 After “surveillance device operations”, insert “and computer data access
12 operations”.

13 **32 Subsection 4(1)**

14 Omit all the words after “Territory,”, substitute:

15 that:

- 16 (a) prohibits or regulates the use of surveillance devices; or
17 (b) prohibits or regulates access to data held in computers.

18 **33 After subsection 4(4)**

19 Insert:

20 (4A) For the avoidance of doubt, it is intended that a warrant may be
21 issued, or an emergency authorisation given, under this Act:

- 22 (a) for access to data held in a computer; and
23 (b) in relation to a relevant offence or a recovery order.

24 **34 After subsection 4(5)**

25 Insert:

26 (5A) For the avoidance of doubt, it is intended that a warrant may be
27 issued under this Act for access to data held in a computer in a case
28 where a control order is in force, and access to the data would be
29 likely to substantially assist in:

- 30 (a) protecting the public from a terrorist act; or
-

- 1 (b) preventing the provision of support for, or the facilitation of,
2 a terrorist act; or
3 (c) preventing the provision of support for, or the facilitation of,
4 the engagement in a hostile activity in a foreign country; or
5 (d) determining whether the control order, or any succeeding
6 control order, has been, or is being, complied with.

7 **35 Subsection 6(1)**

8 Insert:

9 *carrier* means:

- 10 (a) a carrier within the meaning of the *Telecommunications Act*
11 *1997*; or
12 (b) a carriage service provider within the meaning of that Act.

13 *communication in transit* means a communication (within the
14 meaning of the *Telecommunications Act 1997*) passing over a
15 telecommunications network (within the meaning of that Act).

16 **36 Subsection 6(1) (definition of *computer*)**

17 Repeal the definition, substitute:

18 *computer* means all or part of:

- 19 (a) one or more computers; or
20 (b) one or more computer systems; or
21 (c) one or more computer networks; or
22 (d) any combination of the above.

23 **37 Subsection 6(1)**

24 Insert:

25 *computer access warrant* means a warrant issued under
26 section 27C or subsection 35A(4) or (5).

27 *control order access warrant* means a computer access warrant
28 issued in response to an application under subsection 27A(6).

29 *data* includes:

- 30 (a) information in any form; and
31 (b) any program (or part of a program).

1 *data held in a computer* includes:

- 2 (a) data held in any removable data storage device for the time
3 being held in a computer; and
4 (b) data held in a data storage device on a computer network of
5 which the computer forms a part.

6 *data storage device* means a thing (for example, a disk or file
7 server) containing (whether temporarily or permanently), or
8 designed to contain (whether temporarily or permanently), data for
9 use by a computer.

10 **38 Subsection 6(1) (definition of *data surveillance device*)**

11 Omit “a computer”, substitute “an electronic device for storing or
12 processing information”.

13 **39 Subsection 6(1)**

14 Insert:

15 *general computer access intercept information* has the same
16 meaning as in the *Telecommunications (Interception and Access)*
17 *Act 1979*.

18 *intercepting a communication passing over a telecommunications*
19 *system* has the same meaning as in the *Telecommunications*
20 *(Interception and Access) Act 1979*.

21 **40 Subsection 6(1) (definition of *mutual assistance***
22 ***application*)**

23 Repeal the definition, substitute:

24 *mutual assistance application* means:
25 (a) an application for a surveillance device warrant; or
26 (b) an application for a computer access warrant;
27 made under a mutual assistance authorisation.

28 **41 Subsection 6(1) (definition of *mutual assistance***
29 ***authorisation*)**

30 Omit “subsection 15CA(1)”, substitute, “subsection 15CA(1) or
31 15CC(1)”.

1 **42 Subsection 6(1) (paragraph (db) of the definition of**
2 ***relevant offence*)**

3 After “warrant,”, insert “a computer access warrant,”.

4 **43 Subsection 6(1) (definition of *remote application*)**

5 Omit “or 23”, substitute, “, 23 or 27B”.

6 **44 Subsection 6(1)**

7 Insert:

8 *telecommunications facility* means a facility within the meaning of
9 the *Telecommunications Act 1997*.

10 **45 Subsection 6(1) (definition of *unsworn application*)**

11 Omit “or 22(4) and (5)”, substitute “, 22(4) and (5), 27A(9) and (10),
12 27A(11) and (12) or 27A(13) and (14)”.

13 **46 Subsection 6(1) (definition of *warrant*)**

14 Repeal the definition, substitute:

15 *warrant* means:

- 16 (a) a surveillance device warrant; or
17 (b) a retrieval warrant; or
18 (c) a computer access warrant.

19 **47 At the end of subsection 10(1)**

20 Add:

21 ; (c) a computer access warrant.

22 **48 Subsection 10(2)**

23 Before “warrant”, insert “surveillance device warrant or a retrieval”.

24 **49 At the end of Part 2**

25 Add:

1 **Division 4—Computer access warrants**

2 **27A Application for computer access warrant**

3 *Warrants sought for offence investigations*

4 (1) A law enforcement officer (or another person on the law
5 enforcement officer's behalf) may apply for the issue of a
6 computer access warrant if the law enforcement officer suspects on
7 reasonable grounds that:

8 (a) one or more relevant offences have been, are being, are about
9 to be, or are likely to be, committed; and

10 (b) an investigation into those offences is being, will be, or is
11 likely to be, conducted; and

12 (c) access to data held in a computer (the *target computer*) is
13 necessary, in the course of that investigation, for the purpose
14 of enabling evidence to be obtained of:

15 (i) the commission of those offences; or

16 (ii) the identity or location of the offenders.

17 (2) If the application is being made by or on behalf of a State or
18 Territory law enforcement officer, the reference in subsection (1)
19 to a relevant offence does not include a reference to a State offence
20 that has a federal aspect.

21 *Warrants sought for recovery orders*

22 (3) A law enforcement officer (or another person on the law
23 enforcement officer's behalf) may apply for the issue of a
24 computer access warrant if:

25 (a) a recovery order is in force; and

26 (b) the law enforcement officer suspects on reasonable grounds
27 that access to data held in a computer (the *target computer*)
28 may assist in the location and safe recovery of the child to
29 whom the recovery order relates.

1 *Warrants sought for mutual assistance investigations*

- 2 (4) A law enforcement officer (or another person on the law
3 enforcement officer's behalf) may apply for the issue of a
4 computer access warrant if the law enforcement officer:
5 (a) is authorised to do so under a mutual assistance authorisation;
6 and
7 (b) suspects on reasonable grounds that access to data held in a
8 computer (the *target computer*) is necessary, in the course of
9 the investigation or investigative proceeding to which the
10 authorisation relates, for the purpose of enabling evidence to
11 be obtained of:
12 (i) the commission of the offence to which the
13 authorisation relates; or
14 (ii) the identity or location of the persons suspected of
15 committing the offence.

16 *Warrants sought for integrity operations*

- 17 (5) A federal law enforcement officer (or another person on the federal
18 law enforcement officer's behalf) may apply for the issue of a
19 computer access warrant if:
20 (a) an integrity authority is in effect authorising an integrity
21 operation in relation to an offence that it is suspected has
22 been, is being or is likely to be committed by a staff member
23 of a target agency; and
24 (b) the federal law enforcement officer suspects on reasonable
25 grounds that access to data held in a computer (the *target*
26 *computer*) will assist the conduct of the integrity operation
27 by enabling evidence to be obtained relating to the integrity,
28 location or identity of any staff member of the target agency.

29 *Control order access warrants*

- 30 (6) A law enforcement officer (or another person on the law
31 enforcement officer's behalf) may apply for the issue of a
32 computer access warrant if:
33 (a) a control order is in force in relation to a person; and
34 (b) the law enforcement officer suspects on reasonable grounds
35 that access to data held in a computer (the *target computer*)

- 1 to obtain information relating to the person would be likely to
2 substantially assist in:
- 3 (i) protecting the public from a terrorist act; or
 - 4 (ii) preventing the provision of support for, or the
5 facilitation of, a terrorist act; or
 - 6 (iii) preventing the provision of support for, or the
7 facilitation of, the engagement in a hostile activity in a
8 foreign country; or
 - 9 (iv) determining whether the control order, or any
10 succeeding control order, has been, or is being,
11 complied with.

12 Note: For control orders that have been made but not come into force, see
13 section 6C.

14 *Procedure for making applications*

- 15 (7) An application under subsection (1), (3), (4), (5) or (6) may be
16 made to an eligible Judge or to a nominated AAT member.
- 17 (8) An application:
- 18 (a) must specify:
 - 19 (i) the name of the applicant; and
 - 20 (ii) the nature and duration of the warrant sought; and
 - 21 (b) subject to this section, must be supported by an affidavit
22 setting out the grounds on which the warrant is sought.

23 *Unsworn applications—warrants sought for offence investigations*

- 24 (9) If a law enforcement officer believes that:
- 25 (a) immediate access to data held in the target computer referred
26 to in subsection (1) is necessary as described in
27 paragraph (1)(c); and
 - 28 (b) it is impracticable for an affidavit to be prepared or sworn
29 before an application for a warrant is made;
- 30 an application for a warrant under subsection (1) may be made
31 before an affidavit is prepared or sworn.
- 32 (10) If subsection (9) applies, the applicant must:

- 1 (a) provide as much information as the eligible Judge or
2 nominated AAT member considers is reasonably practicable
3 in the circumstances; and
4 (b) not later than 72 hours after the making of the application,
5 send a duly sworn affidavit to the eligible Judge or
6 nominated AAT member, whether or not a warrant has been
7 issued.

8 *Unsworn applications—warrants sought for recovery orders*

- 9 (11) If a law enforcement officer believes that:
10 (a) immediate access to data held in the target computer referred
11 to in subsection (3) may assist as described in
12 paragraph (3)(b); and
13 (b) it is impracticable for an affidavit to be prepared or sworn
14 before an application for a warrant is made;
15 an application for a warrant under subsection (3) may be made
16 before an affidavit is prepared or sworn.
- 17 (12) If subsection (11) applies, the applicant must:
18 (a) provide as much information as the eligible Judge or
19 nominated AAT member considers is reasonably practicable
20 in the circumstances; and
21 (b) not later than 72 hours after the making of the application,
22 send a duly sworn affidavit to the eligible Judge or
23 nominated AAT member, whether or not a warrant has been
24 issued.

25 *Unsworn applications—control order access warrants*

- 26 (13) If a law enforcement officer believes that:
27 (a) immediate access to data held in the target computer referred
28 to in subsection (6) would be likely to substantially assist as
29 described in paragraph (6)(b); and
30 (b) it is impracticable for an affidavit to be prepared or sworn
31 before an application for a warrant is made;
32 an application for a warrant under subsection (6) may be made
33 before an affidavit is prepared or sworn.
- 34 (14) If subsection (13) applies, the applicant must:

- 1 (a) provide as much information as the eligible Judge or
2 nominated AAT member considers is reasonably practicable
3 in the circumstances; and
4 (b) not later than 72 hours after the making of the application,
5 send a duly sworn affidavit to the eligible Judge or
6 nominated AAT member, whether or not a warrant has been
7 issued.

8 *Target computer*

- 9 (15) The target computer referred to in subsection (1), (3), (4), (5) or (6)
10 may be any one or more of the following:
11 (a) a particular computer;
12 (b) a computer on particular premises;
13 (c) a computer associated with, used by or likely to be used by, a
14 person (whose identity may or may not be known).

15 **27B Remote application**

- 16 (1) If a law enforcement officer believes that it is impracticable for an
17 application for a computer access warrant to be made in person, the
18 application may be made under section 27A by telephone, fax,
19 email or any other means of communication.
20 (2) If transmission by fax is available and an affidavit has been
21 prepared, the person applying must transmit a copy of the affidavit,
22 whether sworn or unsworn, to the eligible Judge or to the
23 nominated AAT member who is to determine the application.

24 **27C Determining the application**

- 25 (1) An eligible Judge or a nominated AAT member may issue a
26 computer access warrant if satisfied:
27 (a) in the case of a warrant sought in relation to a relevant
28 offence—that there are reasonable grounds for the suspicion
29 founding the application for the warrant; and
30 (b) in the case of a warrant sought in relation to a recovery
31 order—that such an order is in force and that there are
32 reasonable grounds for the suspicion founding the application
33 for the warrant; and

- 1 (c) in the case of a warrant sought in relation to a mutual
2 assistance authorisation—that such an authorisation is in
3 force and that there are reasonable grounds for the suspicion
4 founding the application for the warrant; and
- 5 (d) in the case of a warrant sought for the purposes of an
6 integrity operation—that the integrity authority for the
7 operation is in effect, and that there are reasonable grounds
8 for the suspicions founding the application for the warrant (as
9 mentioned in paragraphs 27A(5)(a) and (b)); and
- 10 (e) in the case of a control order access warrant—that a control
11 order is in force in relation to a person, and that access to
12 data held in the relevant target computer to obtain
13 information relating to the person would be likely to
14 substantially assist in:
- 15 (i) protecting the public from a terrorist act; or
16 (ii) preventing the provision of support for, or the
17 facilitation of, a terrorist act; or
18 (iii) preventing the provision of support for, or the
19 facilitation of, the engagement in a hostile activity in a
20 foreign country; or
21 (iv) determining whether the control order, or any
22 succeeding control order, has been, or is being,
23 complied with; and
- 24 (f) in the case of an unsworn application—that it would have
25 been impracticable for an affidavit to have been sworn or
26 prepared before the application was made; and
- 27 (g) in the case of a remote application—that it would have been
28 impracticable for the application to have been made in
29 person.

30 Note: For control orders that have been made but not come into force, see
31 section 6C.

- 32 (2) In determining whether a computer access warrant should be
33 issued, the eligible Judge or nominated AAT member must have
34 regard to:
- 35 (a) in the case of a warrant sought in relation to a relevant
36 offence or a mutual assistance authorisation, or for the
37 purposes of an integrity operation—the nature and gravity of
38 the alleged offence; and

- 1 (b) in the case of a warrant sought to assist in the location and
2 safe recovery of a child to whom a recovery order relates—
3 the circumstances that gave rise to the making of the order;
4 and
5 (c) the extent to which the privacy of any person is likely to be
6 affected; and
7 (d) the existence of any alternative means of obtaining the
8 evidence or information sought to be obtained; and
9 (e) in the case of a warrant sought in relation to a relevant
10 offence or a recovery order, or for the purposes of an
11 integrity operation—the likely evidentiary or intelligence
12 value of any evidence or information sought to be obtained;
13 and
14 (f) in the case of a warrant sought in relation to a mutual
15 assistance authorisation—the likely evidentiary or
16 intelligence value of any evidence or information sought to
17 be obtained, to the extent that this is possible to determine
18 from information obtained from the foreign country to which
19 the authorisation relates; and
20 (g) in the case of a control order access warrant issued on the
21 basis of a control order that is in force in relation to a
22 person—the likely value of the information sought to be
23 obtained, in:
24 (i) protecting the public from a terrorist act; or
25 (ii) preventing the provision of support for, or the
26 facilitation of, a terrorist act; or
27 (iii) preventing the provision of support for, or the
28 facilitation of, the engagement in a hostile activity in a
29 foreign country; or
30 (iv) determining whether the control order, or any
31 succeeding control order, has been, or is being,
32 complied with; and
33 (h) in the case of a control order access warrant issued on the
34 basis of a control order that is in force in relation to a
35 person—whether the access to data held in the relevant target
36 computer in accordance with the warrant would be the means
37 of obtaining the evidence or information sought to be
38 obtained, that is likely to have the least interference with any
39 person’s privacy; and
-

- 1 (i) in the case of a control order access warrant issued on the
2 basis of a control order that is in force in relation to a
3 person—the possibility that the person:
4 (i) has engaged, is engaging, or will engage, in a terrorist
5 act; or
6 (ii) has provided, is providing, or will provide, support for a
7 terrorist act; or
8 (iii) has facilitated, is facilitating, or will facilitate, a terrorist
9 act; or
10 (iv) has provided, is providing, or will provide, support for
11 the engagement in a hostile activity in a foreign country;
12 or
13 (v) has facilitated, is facilitating, or will facilitate, the
14 engagement in a hostile activity in a foreign country; or
15 (vi) has contravened, is contravening, or will contravene, the
16 control order; or
17 (vii) will contravene a succeeding control order; and
18 (j) in the case of a warrant sought in relation to a relevant
19 offence or a recovery order—any previous warrant sought or
20 issued under this Division in connection with the same
21 alleged offence or the same recovery order; and
22 (k) in the case of a control order access warrant issued on the
23 basis of a control order that is in force in relation to a
24 person—any previous control order access warrant sought or
25 issued on the basis of a control order relating to the person.

26 **27D What must a computer access warrant contain?**

- 27 (1) A computer access warrant must:
28 (a) state that the eligible Judge or nominated AAT member
29 issuing the warrant is satisfied of the matters referred to in
30 subsection 27C(1) and has had regard to the matters referred
31 to in subsection 27C(2); and
32 (b) specify:
33 (i) the name of the applicant; and
34 (ii) if the warrant relates to one or more alleged relevant
35 offences—the alleged offences in respect of which the
36 warrant is issued; and

- 1 (iii) if the warrant relates to a recovery order—the date the
2 order was made and the name of the child to whom the
3 order relates; and
- 4 (iv) if the warrant relates to a mutual assistance
5 authorisation—the offence or offences against the law
6 of a foreign country to which the authorisation relates;
7 and
- 8 (v) if the warrant is issued for the purposes of an integrity
9 operation—the integrity authority for the operation and
10 each alleged relevant offence in relation to which the
11 authority was granted; and
- 12 (vi) the date the warrant is issued; and
- 13 (vii) if the target computer is or includes a particular
14 computer—the computer; and
- 15 (viii) if the target computer is or includes a computer on
16 particular premises—the premises; and
- 17 (ix) if the target computer is or includes a computer
18 associated with, used by or likely to be used by, a
19 person—the person (whether by name or otherwise);
20 and
- 21 (x) the period during which the warrant is in force (see
22 subsection (3)); and
- 23 (xi) the name of the law enforcement officer primarily
24 responsible for executing the warrant; and
- 25 (xii) any conditions subject to which things may be done
26 under the warrant.
- 27 (2) If a control order access warrant is issued on the basis of a control
28 order that is in force in relation to a person, the warrant must also
29 specify the following details in relation to the control order:
- 30 (a) the name of the person;
- 31 (b) the date the control order was made;
- 32 (c) whether the control order is an interim control order or a
33 confirmed control order.
- 34 (3) A warrant may only be issued:
- 35 (a) for a period of no more than 90 days; or
- 36 (b) if the warrant is issued for the purposes of an integrity
37 operation—for a period of no more than 21 days.
-

1 Note: The access to data held in the target computer pursuant to a warrant
2 may be discontinued earlier—see section 27H.

3 (4) In the case of a warrant authorising the access to data held in the
4 target computer on premises that are vehicles, the warrant need
5 only specify the class of vehicle in relation to which the access to
6 data held in the target computer is authorised.

7 (5) A warrant must be signed by the person issuing it and include the
8 person's name.

9 (6) As soon as practicable after completing and signing a warrant
10 issued on a remote application, the person issuing it must:
11 (a) inform the applicant of:
12 (i) the terms of the warrant; and
13 (ii) the date on which, and the time at which, the warrant
14 was issued; and
15 (b) give the warrant to the applicant while retaining a copy of the
16 warrant for the person's own record.

17 **27E What a computer access warrant authorises**

18 (1) A computer access warrant must authorise the doing of specified
19 things (subject to any restrictions or conditions specified in the
20 warrant) in relation to the relevant target computer.

21 (2) The things that may be specified are any of the following that the
22 eligible Judge or nominated AAT member considers appropriate in
23 the circumstances:

- 24 (a) entering specified premises for the purposes of doing the
25 things mentioned in this subsection;
- 26 (b) entering any premises for the purposes of gaining entry to, or
27 exiting, the specified premises;
- 28 (c) using:
- 29 (i) the target computer; or
- 30 (ii) a telecommunications facility operated or provided by
31 the Commonwealth or a carrier; or
- 32 (iii) any other electronic equipment; or
- 33 (iv) a data storage device;

- 1 for the purpose of obtaining access to data (the *relevant data*)
2 that is held in the target computer at any time while the
3 warrant is in force, in order to determine whether the relevant
4 data is covered by the warrant;
- 5 (d) if necessary to achieve the purpose mentioned in
6 paragraph (c)—adding, copying, deleting or altering other
7 data in the target computer;
- 8 (e) if, having regard to other methods (if any) of obtaining access
9 to the relevant data which are likely to be as effective, it is
10 reasonable in all the circumstances to do so:
- 11 (i) using any other computer or a communication in transit
12 to access the relevant data; and
- 13 (ii) if necessary to achieve that purpose—adding, copying,
14 deleting or altering other data in the computer or the
15 communication in transit;
- 16 (f) removing a computer or other thing from premises for the
17 purposes of doing any thing specified in the warrant in
18 accordance with this subsection, and returning the computer
19 or other thing to the premises;
- 20 (g) copying any data to which access has been obtained, and that:
- 21 (i) appears to be relevant for the purposes of determining
22 whether the relevant data is covered by the warrant; or
23 (ii) is covered by the warrant;
- 24 (h) intercepting a communication passing over a
25 telecommunications system, if the interception is for the
26 purposes of doing any thing specified in the warrant in
27 accordance with this subsection;
- 28 (i) any other thing reasonably incidental to any of the above.

29 Note: As a result of the warrant, a person who, by means of a
30 telecommunications facility, obtains access to data stored in a
31 computer etc. will not commit an offence under Part 10.7 of the
32 *Criminal Code* or equivalent State or Territory laws (provided that the
33 person acts within the authority of the warrant).

34 (2A) If:

- 35 (a) a computer access warrant authorises the removal of a
36 computer or other thing from premises as mentioned in
37 paragraph (2)(f); and

1 (b) a computer or thing is removed from the premises in
2 accordance with the warrant;
3 the computer or thing must be returned to the premises within a
4 reasonable period.

5 (3) For the purposes of paragraph (2)(g), if:
6 (a) access has been obtained to data; and
7 (b) the data is subject to a form of electronic protection;
8 the data is taken to be relevant for the purposes of determining
9 whether the relevant data is covered by the warrant.

10 *When data is covered by a warrant*

11 (4) For the purposes of this section, data is **covered by** a warrant if:
12 (a) in the case of a warrant sought in relation to a relevant
13 offence—access to the data is necessary as described in
14 paragraph 27A(1)(c); or
15 (b) in the case of a warrant sought in relation to a recovery
16 order—access to the data may assist as described in
17 paragraph 27A(3)(b); or
18 (c) in the case of a warrant sought in relation to a mutual
19 assistance authorisation—access to the data is necessary as
20 described in paragraph 27A(4)(b); or
21 (d) in the case of a warrant sought for the purposes of an
22 integrity operation—access to the data will assist as
23 described in paragraph 27A(5)(b); or
24 (e) in the case of a control order access warrant—access to the
25 data would be likely to substantially assist as described in
26 paragraph 27A(6)(b).

27 *Certain acts not authorised*

28 (5) Subsection (2) does not authorise the addition, deletion or
29 alteration of data, or the doing of any thing, that is likely to:
30 (a) materially interfere with, interrupt or obstruct:
31 (i) a communication in transit; or
32 (ii) the lawful use by other persons of a computer;

1 unless the addition, deletion or alteration, or the doing of the
2 thing, is necessary to do one or more of the things specified
3 in the warrant; or

4 (b) cause any other material loss or damage to other persons
5 lawfully using a computer.

6 *Warrant must provide for certain matters*

7 (6) A computer access warrant must:

8 (a) authorise the use of any force against persons and things that
9 is necessary and reasonable to do the things specified in the
10 warrant; and

11 (b) if the warrant authorises entering premises—state whether
12 entry is authorised to be made at any time of the day or night
13 or during stated hours of the day or night.

14 *Concealment of access etc.*

15 (7) If any thing has been done in relation to a computer under:

16 (a) a computer access warrant; or

17 (b) this subsection;

18 then, in addition to the things specified in the warrant, the warrant
19 authorises the doing of any of the following:

20 (c) any thing reasonably necessary to conceal the fact that any
21 thing has been done under the warrant or under this
22 subsection;

23 (d) entering any premises where the computer is reasonably
24 believed to be, for the purposes of doing the things
25 mentioned in paragraph (c);

26 (e) entering any other premises for the purposes of gaining entry
27 to or exiting the premises referred to in paragraph (d);

28 (f) removing the computer or another thing from any place
29 where it is situated for the purposes of doing the things
30 mentioned in paragraph (c), and returning the computer or
31 other thing to that place;

32 (g) if, having regard to other methods (if any) of doing the things
33 mentioned in paragraph (c) which are likely to be as
34 effective, it is reasonable in all the circumstances to do so:

- 1 (i) using any other computer or a communication in transit
2 to do those things; and
3 (ii) if necessary to achieve that purpose—adding, copying,
4 deleting or altering other data in the computer or the
5 communication in transit;
- 6 (h) intercepting a communication passing over a
7 telecommunications system, if the interception is for the
8 purposes of doing any thing mentioned in this subsection;
- 9 (i) any other thing reasonably incidental to any of the above;
10 at the following time:
- 11 (j) at any time while the warrant is in force or within 28 days
12 after it ceases to be in force;
- 13 (k) if none of the things mentioned in paragraph (c) are done
14 within the 28-day period mentioned in paragraph (j)—at the
15 earliest time after that 28-day period at which it is reasonably
16 practicable to do the things mentioned in paragraph (c).
- 17 (8) Subsection (7) does not authorise the doing of a thing that is likely
18 to:
- 19 (a) materially interfere with, interrupt or obstruct:
20 (i) a communication in transit; or
21 (ii) the lawful use by other persons of a computer;
22 unless the doing of the thing is necessary to do one or more
23 of the things specified in subsection (7); or
24 (b) cause any other material loss or damage to other persons
25 lawfully using a computer.
- 26 (9) If a computer or another thing is removed from a place in
27 accordance with paragraph (7)(f), the computer or thing must be
28 returned to the place within a reasonable period.

29 **27F Extension and variation of computer access warrant**

- 30 (1) A law enforcement officer to whom a computer access warrant has
31 been issued (or another person on the law enforcement officer's
32 behalf) may apply, at any time before the expiry of the warrant:
33 (a) for an extension of the warrant for a period of no more than:
34 (i) 90 days after the day the warrant would otherwise
35 expire; or
-

- 1 (ii) if the warrant is issued for the purposes of an integrity
2 operation—21 days after the day the warrant would
3 otherwise expire; or
4 (b) for a variation of any of the other terms of the warrant.
- 5 (2) The application is to be made to an eligible Judge or to a
6 nominated AAT member and must be accompanied by the original
7 warrant.
- 8 (3) Sections 27A and 27B apply, with any necessary changes, to an
9 application under this section as if it were an application for the
10 warrant.
- 11 (4) The eligible Judge or nominated AAT member may grant an
12 application if satisfied that the matters referred to in
13 subsection 27C(1) still exist, having regard to the matters in
14 subsection 27C(2).
- 15 (5) If the eligible Judge or nominated AAT member grants the
16 application, the eligible Judge or nominated AAT member must
17 endorse the new expiry date or the other varied term on the original
18 warrant.
- 19 (6) An application may be made under this section more than once.

20 **27G Revocation of computer access warrant**

- 21 (1) A computer access warrant may, by instrument in writing, be
22 revoked by an eligible Judge or nominated AAT member on the
23 initiative of the eligible Judge or nominated AAT member at any
24 time before the expiration of the period of validity specified in the
25 warrant.
- 26 (2) If the circumstances set out in paragraphs 27H(2)(a) and (b),
27 27H(3)(a) and (b), 27H(4)(a) and (b), 27H(5)(a) and (b), 27H(6)(a)
28 and (b) or 27H(7)(a) and (b) apply in relation to a computer access
29 warrant, the chief officer of the law enforcement agency to which
30 the law enforcement officer to whom the warrant was issued
31 belongs or is seconded must, by instrument in writing, revoke the
32 warrant.

- 1 (3) The instrument revoking a warrant must be signed by the eligible
2 Judge, the nominated AAT member or the chief officer of the law
3 enforcement agency, as the case requires.
- 4 (4) If an eligible Judge or nominated AAT member revokes a warrant,
5 the eligible Judge or nominated AAT member must give a copy of
6 the instrument of revocation to the chief officer of the law
7 enforcement agency to which the law enforcement officer to whom
8 the warrant was issued belongs or is seconded.
- 9 (5) If:
- 10 (a) an eligible Judge or nominated AAT member revokes a
11 warrant; and
- 12 (b) at the time of the revocation, a law enforcement officer is
13 executing the warrant;
- 14 the law enforcement officer is not subject to any civil or criminal
15 liability for any act done in the proper execution of that warrant
16 before the officer is made aware of the revocation.

17 **27H Discontinuance of access under warrant**

18 *Scope*

- 19 (1) This section applies if a computer access warrant is issued to a law
20 enforcement officer.

21 *Discontinuance of access*

- 22 (2) If:
- 23 (a) the computer access warrant has been sought by or on behalf
24 of a law enforcement officer in relation to a relevant offence;
25 and
- 26 (b) the chief officer of the law enforcement agency to which the
27 law enforcement officer belongs or is seconded is satisfied
28 that access to data under the warrant is no longer required for
29 the purpose of enabling evidence to be obtained of:
- 30 (i) the commission of the relevant offence; or
31 (ii) the identity or location of the offender;

1 the chief officer must, in addition to revoking the warrant under
2 section 27G, take the steps necessary to ensure that access to data
3 authorised by the warrant is discontinued.

4 (3) If:

5 (a) the computer access warrant has been sought by or on behalf
6 of a law enforcement officer in relation to a recovery order;
7 and

8 (b) the chief officer of the law enforcement agency to which the
9 law enforcement officer belongs or is seconded is satisfied
10 that access to data under the warrant is no longer required for
11 the purpose of locating and safely recovering the child to
12 whom the recovery order relates;

13 the chief officer must, in addition to revoking the warrant under
14 section 27G, take the steps necessary to ensure that access to data
15 authorised by the warrant is discontinued.

16 (4) If:

17 (a) the computer access warrant has been sought by or on behalf
18 of a law enforcement officer as authorised under a mutual
19 assistance authorisation; and

20 (b) the chief officer of the law enforcement agency to which the
21 law enforcement officer belongs or is seconded is satisfied
22 that access to data under the warrant is no longer required for
23 the purpose of enabling evidence to be obtained of:

24 (i) the commission of the offence against a law of a foreign
25 country to which the authorisation relates; or

26 (ii) the identity or location of the persons suspected of
27 committing the offence;

28 the chief officer must, in addition to revoking the warrant under
29 section 27G, take the steps necessary to ensure that access to data
30 authorised by the warrant is discontinued.

31 (5) If:

32 (a) the computer access warrant has been sought by or on behalf
33 of a federal law enforcement officer for the purposes of an
34 integrity operation; and

35 (b) the chief officer of the law enforcement agency to which the
36 law enforcement officer belongs or is seconded is satisfied
37 that:

1 (i) access to data under the warrant is no longer necessary
2 for the purposes of the integrity operation; or
3 (ii) the integrity authority for the integrity operation is no
4 longer in effect;
5 the chief officer must, in addition to revoking the warrant under
6 section 27G, take the steps necessary to ensure access to data
7 authorised by the warrant is discontinued.

8 (6) If:
9 (a) the computer access warrant is a control order access warrant
10 issued on the basis of a control order that was in force in
11 relation to a person; and
12 (b) the chief officer of the law enforcement agency to which the
13 law enforcement officer belongs or is seconded is satisfied
14 that access to data under the warrant to obtain information
15 relating to the person is no longer required for any of the
16 following purposes:
17 (i) protecting the public from a terrorist act;
18 (ii) preventing the provision of support for, or the
19 facilitation of, a terrorist act;
20 (iii) preventing the provision of support for, or the
21 facilitation of, the engagement in a hostile activity in a
22 foreign country;
23 (iv) determining whether the control order, or any
24 succeeding control order, has been, or is being,
25 complied with;

26 the chief officer must, in addition to revoking the warrant under
27 section 27G, take the steps necessary to ensure that access to data
28 authorised by the warrant is discontinued as soon as practicable.

29 (7) If:
30 (a) the computer access warrant is a control order access warrant
31 issued on the basis of a control order that was in force in
32 relation to a person; and
33 (b) no control order is in force in relation to the person;
34 the chief officer must, in addition to revoking the warrant under
35 section 27G, take the steps necessary to ensure that access to data
36 authorised by the warrant is discontinued as soon as practicable.

- 1 (8) If the chief officer of a law enforcement agency is notified that a
2 warrant has been revoked by an eligible Judge or a nominated
3 AAT member under section 27G, the eligible Judge or nominated
4 AAT member must take the steps necessary to ensure that access to
5 data authorised by the warrant is discontinued as soon as
6 practicable.
- 7 (9) If the law enforcement officer to whom the warrant is issued, or
8 who is primarily responsible for executing the warrant, believes
9 that access to data under the warrant is no longer necessary for the
10 purpose:
- 11 (a) if the warrant was issued in relation to a relevant offence—of
12 enabling evidence to be obtained of the commission of the
13 relevant offence or the identity or location of the offender; or
14 (b) if the warrant was issued in relation to a recovery order—of
15 enabling the location and safe recovery of the child to whom
16 the order relates; or
17 (c) if the warrant was issued in relation to a mutual assistance
18 authorisation—of enabling evidence to be obtained of:
- 19 (i) the commission of the offence against a law of a foreign
20 country to which the authorisation relates; or
21 (ii) the identity or location of the persons suspected of
22 committing the offence;
- 23 the law enforcement officer must immediately inform the chief
24 officer of the law enforcement agency to which the law
25 enforcement officer belongs or is seconded.
- 26 (10) In the case of a warrant issued for the purposes of an integrity
27 operation, if the law enforcement officer to whom the warrant is
28 issued, or who is primarily responsible for executing the warrant,
29 believes that:
- 30 (a) access to data under the warrant is no longer necessary for
31 those purposes; or
32 (b) the integrity authority for the integrity operation is no longer
33 in effect;
- 34 the law enforcement officer must immediately inform the chief
35 officer of the law enforcement agency to which the law
36 enforcement officer belongs or is seconded.
-

1 **27J Relationship of this Division to parliamentary privileges and**
2 **immunities**

3 To avoid doubt, this Division does not affect the law relating to the
4 powers, privileges and immunities of any of the following:

- 5 (a) each House of the Parliament;
6 (b) the members of each House of the Parliament;
7 (c) the committees of each House of the Parliament and joint
8 committees of both Houses of the Parliament.

9 **50 After subsection 28(1)**

10 Insert:

11 (1A) A law enforcement officer may apply to an appropriate authorising
12 officer for an emergency authorisation for access to data held in a
13 computer (the *target computer*) if, in the course of an investigation
14 of a relevant offence, the law enforcement officer reasonably
15 suspects that:

- 16 (a) an imminent risk of serious violence to a person or
17 substantial damage to property exists; and
18 (b) access to data held in the target computer is immediately
19 necessary for the purpose of dealing with that risk; and
20 (c) the circumstances are so serious and the matter is of such
21 urgency that access to data held in the target computer is
22 warranted; and
23 (d) it is not practicable in the circumstances to apply for a
24 computer access warrant.

25 (1B) The target computer may be any one or more of the following:

- 26 (a) a particular computer;
27 (b) a computer on particular premises;
28 (c) a computer associated with, used by or likely to be used by, a
29 person (whose identity may or may not be known).

30 **51 Subsections 28(2), (3) and (4)**

31 After “application”, insert “mentioned in subsection (1) or (1A)”.

32 **52 After subsection 29(1)**

33 Insert:

1 (1A) A law enforcement officer may apply to an appropriate authorising
2 officer for an emergency authorisation for access to data held in a
3 computer (the *target computer*) if:

- 4 (a) a recovery order is in force; and
5 (b) the law enforcement officer reasonably suspects that:
6 (i) the circumstances are so urgent as to warrant immediate
7 access to data held in the target computer; and
8 (ii) it is not practicable in the circumstances to apply for a
9 computer access warrant.

10 (1B) The target computer may be any one or more of the following:

- 11 (a) a particular computer;
12 (b) a computer on particular premises;
13 (c) a computer associated with, used by or likely to be used by, a
14 person (whose identity may or may not be known).

15 **53 Subsections 29(2) and (3)**

16 After “application”, insert “mentioned in subsection (1) or (1A)”.

17 **54 After subsection 30(1)**

18 Insert:

19 (1A) If:

- 20 (a) a law enforcement officer is conducting an investigation into:
21 (i) an offence against section 233BAA of the *Customs Act*
22 *1901* (with respect to goods listed in Schedule 4 to the
23 *Customs (Prohibited Imports) Regulations 1956* or in
24 Schedule 8 or 9 to the *Customs (Prohibited Exports)*
25 *Regulations 1958*); or
26 (ii) an offence under the *Crimes (Traffic in Narcotic Drugs*
27 *and Psychotropic Substances) Act 1990* or an offence
28 against Part 9.1 of the *Criminal Code* (other than
29 section 308.1 or 308.2); or
30 (iii) an offence against section 73.2 or 73.3 or Division 91 of
31 the *Criminal Code*; or
32 (iv) an offence under Subdivision A of Division 72 or
33 Division 80, 101, 102, 103, 270, 272 or 273 of the
34 *Criminal Code*; or

- 1 (v) an offence against section 233B or 233C of the
2 *Migration Act 1958*;
3 or more than one offence; and
4 (b) the law enforcement officer reasonably suspects that:
5 (i) access to data held in a computer (the *target computer*)
6 is immediately necessary to prevent the loss of any
7 evidence relevant to that investigation; and
8 (ii) the circumstances are so serious and the matter is of
9 such urgency that access to data held in the target
10 computer is warranted; and
11 (iii) it is not practicable in the circumstances to apply for a
12 computer access warrant;
13 the law enforcement officer may apply to an appropriate
14 authorising officer for an emergency authorisation for access to
15 data held in the target computer.
- 16 (1B) The target computer may be any one or more of the following:
17 (a) a particular computer;
18 (b) a computer on particular premises;
19 (c) a computer associated with, used by or likely to be used by, a
20 person (whose identity may or may not be known).

21 **55 Subsection 30(2)**

22 After “application”, insert “mentioned in subsection (1) or (1A)”.

23 **56 Subsection 30(3)**

24 Omit “The”, substitute “In the case of an application mentioned in
25 subsection (1), the”.

26 **57 At the end of section 30**

27 Add:

- 28 (4) In the case of an application mentioned in subsection (1A), the
29 appropriate authorising officer may give the emergency
30 authorisation if satisfied that:
31 (a) an investigation is being conducted into an offence referred
32 to in paragraph (1A)(a); and
33 (b) there are reasonable grounds for the suspicion referred to in
34 paragraph (1A)(b).
-

1 **58 Subsections 32(1) and (2)**

2 After “authorisation”, insert “for the use of a surveillance device”.

3 **59 After subsection 32(2)**

4 Insert:

5 (2A) An emergency authorisation for access to data held in a computer
6 may authorise anything that a computer access warrant may
7 authorise.

8 **60 After subsection 32(3)**

9 Insert:

10 (3A) A law enforcement officer may, under an emergency authorisation,
11 access data held in a computer only if the officer is acting in the
12 performance of the officer’s duty.

13 **60A Subsection 32(4)**

14 After “this Part”, insert “(other than subsection (2A) of this section)”.

15 **61 Subsection 33(2)**

16 Omit “The”, substitute “In the case of an application for an emergency
17 authorisation for the use of a surveillance device, the”.

18 **62 After subsection 33(2)**

19 Insert:

20 (2A) In the case of an application for an emergency authorisation for
21 access to data held in a computer, the application:
22 (a) must specify:
23 (i) the name of the applicant for the approval; and
24 (ii) if a warrant is sought—the nature and duration of the
25 warrant; and
26 (b) must be supported by an affidavit setting out the grounds on
27 which the approval (and warrant, if any) is sought; and
28 (c) must be accompanied by a copy of the written record made
29 under section 31 in relation to the emergency authorisation.

1 **63 Subsection 34(1)**

2 Omit “section 28”, substitute “subsection 28(1)”.

3 **64 After subsection 34(1)**

4 Insert:

5 (1A) Before deciding an application for approval of the giving of an
6 emergency authorisation given in response to an application under
7 subsection 28(1A), the eligible Judge or nominated AAT member
8 considering the application must, in particular, and being mindful
9 of the intrusive nature of accessing data held in the target computer
10 mentioned in that subsection, consider the following:

- 11 (a) the nature of the risk of serious violence to a person or
12 substantial damage to property;
- 13 (b) the extent to which issuing a computer access warrant would
14 have helped reduce or avoid the risk;
- 15 (c) the extent to which law enforcement officers could have used
16 alternative methods of investigation to help reduce or avoid
17 the risk;
- 18 (d) how much the use of alternative methods of investigation
19 could have helped reduce or avoid the risk;
- 20 (e) how much the use of alternative methods of investigation
21 would have prejudiced the safety of the person or property
22 because of delay or for another reason;
- 23 (f) whether or not it was practicable in the circumstances to
24 apply for a computer access warrant.

25 **65 Subsection 34(2)**

26 Omit “section 29”, substitute “subsection 29(1)”.

27 **66 After subsection 34(2)**

28 Insert:

29 (2A) Before deciding an application for approval of the giving of an
30 emergency authorisation given in response to an application under
31 subsection 29(1A), the eligible Judge or nominated AAT member
32 considering the application must, in particular, and being mindful
33 of the intrusive nature of accessing data held in the target computer
34 mentioned in that subsection, consider the following:

- 1 (a) the urgency of enforcing the recovery order;
- 2 (b) the extent to which access to data held in the target computer
- 3 mentioned in that subsection would assist in the location and
- 4 safe recovery of the child to whom the recovery order relates;
- 5 (c) the extent to which law enforcement officers could have used
- 6 alternative methods to assist in the location and safe recovery
- 7 of the child;
- 8 (d) how much the use of alternative methods to assist in the
- 9 location and safe recovery of the child might have prejudiced
- 10 the effective enforcement of the recovery order;
- 11 (e) whether or not it was practicable in the circumstances to
- 12 apply for a computer access warrant.

13 **67 Subsection 34(3)**

14 Omit “section 30”, substitute “subsection 30(1)”.

15 **68 At the end of section 34**

16 Add:

- 17 (4) Before deciding an application for approval of the giving of an
- 18 emergency authorisation given in response to an application under
- 19 subsection 30(1A), the eligible Judge or nominated AAT member
- 20 must, in particular, and being mindful of the intrusive nature of
- 21 accessing data held in the target computer mentioned in that
- 22 subsection, consider the following:
- 23 (a) the nature of the risk of the loss of evidence;
- 24 (b) the extent to which issuing a computer access warrant would
- 25 have helped reduce or avoid the risk;
- 26 (c) the extent to which law enforcement officers could have used
- 27 alternative methods of investigation to help reduce or avoid
- 28 the risk;
- 29 (d) how much the use of alternative methods of investigation
- 30 could have helped reduce or avoid the risk;
- 31 (e) whether or not it was practicable in the circumstances to
- 32 apply for a computer access warrant.

33 **69 Section 35 (heading)**

34 Repeal the heading, substitute:

1 **35 Judge or nominated AAT member may approve giving of an**
2 **emergency authorisation for the use of a surveillance**
3 **device**

4 **70 Subsection 35(1)**

5 Omit “under section 28”, substitute “in response to an application under
6 subsection 28(1)”.

7 **71 Subsection 35(1)**

8 Omit “approve the application”, substitute “give the approval”.

9 **72 Subsection 35(2)**

10 Omit “under section 29”, substitute “in response to an application under
11 subsection 29(1)”.

12 **73 Subsection 35(2)**

13 Omit “approve the application”, substitute “give the approval”.

14 **74 Subsection 35(3)**

15 Omit “under section 30”, substitute “in response to an application under
16 subsection 30(1)”.

17 **75 Subsection 35(3)**

18 Omit “approve the application”, substitute “give the approval”.

19 **76 After section 35**

20 Insert:

21 **35A Judge or nominated AAT member may approve giving of an**
22 **emergency authorisation for access to data held in a**
23 **computer**

24 (1) After considering an application for approval of the giving of an
25 emergency authorisation in response to an application under
26 subsection 28(1A), the eligible Judge or nominated AAT member
27 may give the approval if satisfied that there were reasonable
28 grounds to suspect that:

- 1 (a) there was a risk of serious violence to a person or substantial
2 damage to property; and
- 3 (b) accessing data held in the target computer mentioned in that
4 subsection may have helped reduce the risk; and
- 5 (c) it was not practicable in the circumstances to apply for a
6 computer access warrant.
- 7 (2) After considering an application for approval of the giving of an
8 emergency authorisation in response to an application under
9 subsection 29(1A) in relation to a recovery order, the eligible
10 Judge or nominated AAT member may give the approval if
11 satisfied that:
- 12 (a) the recovery order was in force at the time the emergency
13 authorisation was given; and
- 14 (b) there were reasonable grounds to suspect that:
- 15 (i) the enforcement of the recovery order was urgent; and
- 16 (ii) accessing data held in the target computer mentioned in
17 that subsection may have assisted in the prompt location
18 and safe recovery of the child to whom the order relates;
19 and
- 20 (iii) it was not practicable in the circumstances to apply for a
21 computer access warrant.
- 22 (3) After considering an application for approval of the giving of an
23 emergency authorisation in response to an application under
24 subsection 30(1A), the eligible Judge or nominated AAT member
25 may give the approval if satisfied that:
- 26 (a) there were reasonable grounds to suspect that:
- 27 (i) there was a risk of loss of evidence; and
- 28 (ii) accessing data held in the target computer mentioned in
29 that subsection may have helped reduce the risk; and
- 30 (b) it was not practicable in the circumstances to apply for a
31 computer access warrant.
- 32 (4) If, under subsection (1), (2) or (3), the eligible Judge or nominated
33 AAT member approves the giving of an emergency authorisation,
34 the eligible Judge or nominated AAT member may:
- 35 (a) unless paragraph (b) applies—issue a computer access
36 warrant relating to the continued access to data held in the
-

- 1 relevant target computer as if the application for the approval
2 were an application for a computer access warrant under
3 Division 4 of Part 2; or
- 4 (b) if the eligible Judge or nominated AAT member is satisfied
5 that, since the application for the emergency authorisation,
6 the activity that required access to data held in the relevant
7 target computer has ceased—order that access to data held in
8 that computer cease.
- 9 (5) If, under subsection (1), (2) or (3), the eligible Judge or nominated
10 AAT member does not approve the giving of an emergency
11 authorisation, the eligible Judge or nominated AAT member may:
- 12 (a) order that access to data held in the relevant target computer
13 cease; or
- 14 (b) if the eligible Judge or nominated AAT member is of the
15 view that, although the situation did not warrant the
16 emergency authorisation at the time that authorisation was
17 given, the use of a computer access warrant under Division 4
18 of Part 2 is currently justified—issue a computer access
19 warrant relating to the subsequent access to such data as if
20 the application for the approval were an application for a
21 computer access warrant under Division 4 of Part 2.
- 22 (6) In any case, the eligible Judge or nominated AAT member may
23 order that any information obtained from or relating to the exercise
24 of powers under the emergency authorisation, or any record of that
25 information, be dealt with in a manner specified in the order, so
26 long as the manner does not involve the destruction of that
27 information.

28 **77 Section 36**

29 After “section 35”, insert “or 35A”.

30 **78 Section 41 (definition of *appropriate consenting official*)**

31 Repeal the definition, substitute:

32 *appropriate consenting official*, in relation to a foreign country:

- 33 (a) when used in section 42 or 43—means an official of that
34 country having authority in that country to give consent to

1 the use of surveillance devices in that country or on a vessel
2 or aircraft registered under the laws of that country; or
3 (b) when used in section 43A or 43B—means an official of that
4 country having authority in that country to give consent to
5 access to data held in computers in that country or on a vessel
6 or aircraft registered under the laws of that country.

7 **79 Section 42 (heading)**

8 Repeal the heading, substitute:

9 **42 Extraterritorial operation of surveillance device warrants**

10 **80 Subsection 42(1)**

11 Before “warrant” (first occurring), insert “surveillance device”.

12 **81 After paragraph 42(2)(a)**

13 Insert:

14 (aa) the emergency authorisation was given in response to an
15 application under subsection 28(1); and

16 **82 Paragraph 42(2)(b)**

17 After “of that”, insert “section 33”.

18 **83 Subsection 42(2)**

19 After “whom the”, insert “section 33”.

20 **84 Subsection 42(2)**

21 After “consideration of that”, insert “section 33”.

22 **85 Paragraph 42(3)(a)**

23 Before “warrant”, insert “surveillance device”.

24 **86 Subsections 42(6) and (9)**

25 Before “warrant” (first occurring), insert “surveillance device”.

26 **87 At the end of Part 5**

27 Add:

1 **43A Extraterritorial operation of computer access warrants**

2 (1) If, before the issue of a computer access warrant in relation to the
3 investigation of a relevant offence in response to an application
4 made by or on behalf of a federal law enforcement officer, it
5 becomes apparent to the applicant that there will be a need for
6 access to data held in a computer:

7 (a) in a foreign country; or

8 (b) on a vessel or aircraft that is registered under the law of a
9 foreign country and is in or above waters beyond the outer
10 limits of the territorial sea of Australia;

11 to assist in that investigation, the eligible Judge or nominated AAT
12 member considering the application for the warrant must not
13 permit the warrant to authorise that access unless the eligible Judge
14 or nominated AAT member is satisfied that the access has been
15 agreed to by an appropriate consenting official of the foreign
16 country.

17 (2) If:

18 (a) application is made under section 33 by an appropriate
19 authorising officer who is a federal law enforcement officer
20 for approval of the giving of an emergency authorisation
21 relating to the investigation of a relevant offence; and

22 (b) the emergency authorisation was given in response to an
23 application under subsection 28(1A); and

24 (c) before the completion of consideration of that section 33
25 application, it becomes apparent to the applicant that there
26 will be a need for access to data held in a computer:

27 (i) in a foreign country; or

28 (ii) on a vessel or aircraft that is registered under the law of
29 a foreign country and is in or above waters beyond the
30 outer limits of the territorial sea of Australia;

31 to assist in the investigation to which the emergency
32 authorisation related;

33 the eligible Judge or nominated AAT member to whom the
34 section 33 application was made must not permit any computer
35 access warrant issued on consideration of that section 33
36 application to authorise that access unless the eligible Judge or
37 nominated AAT member is satisfied that the access has been

- 1 agreed to by an appropriate consenting official of the foreign
2 country.
- 3 (3) If:
- 4 (a) a computer access warrant has been issued in relation to the
5 investigation of a relevant offence in response to an
6 application by or on behalf of a federal law enforcement
7 officer; and
- 8 (b) after the issue of the warrant, it becomes apparent to the law
9 enforcement officer primarily responsible for executing the
10 warrant that there will be a need for access to data held in a
11 computer that is:
- 12 (i) in a foreign country; or
- 13 (ii) on a vessel or aircraft that is registered under the law of
14 a foreign country and is in or above waters beyond the
15 outer limits of the territorial sea of Australia;
- 16 to assist in that investigation;
- 17 the warrant is taken to permit that access if, and only if, the access
18 has been agreed to by an appropriate consenting official of the
19 foreign country.
- 20 (4) Subsections (1), (2) and (3) do not apply to a computer access
21 warrant authorising access to data if:
- 22 (a) the person, or each of the persons, responsible for executing
23 the warrant will be physically present in Australia; and
- 24 (b) the location where the data is held is unknown or cannot
25 reasonably be determined.
- 26 (5) Despite subsections (1), (2) and (3), if:
- 27 (a) a vessel that is registered under the law of a foreign country
28 is in waters beyond the outer limits of the territorial sea of
29 Australia but not beyond the outer limits of the contiguous
30 zone of Australia; and
- 31 (b) the relevant offence in respect of which it becomes apparent
32 that access to data held in a computer on the vessel will be
33 required is an offence relating to the customs, fiscal,
34 immigration or sanitary laws of Australia;
- 35 there is no requirement for the agreement of an appropriate
36 consenting official of the foreign country concerned in relation to
37 that access while the vessel is in such waters.
-

- 1 (6) Despite subsections (1), (2) and (3), if:
2 (a) a vessel that is registered under the law of a foreign country
3 is in waters beyond the outer limits of the territorial sea of
4 Australia but not beyond the outer limits of the Australian
5 fishing zone; and
6 (b) the relevant offence in respect of which it becomes apparent
7 that access to data held in a computer on the vessel will be
8 required is an offence against section 100, 100A, 100B, 101,
9 101A or 101AA of the *Fisheries Management Act 1991* or
10 section 46A, 46B, 46C, 46D, 49A or 51A of the *Torres Strait*
11 *Fisheries Act 1984*;
12 there is no requirement for the agreement of an appropriate
13 consenting official of the foreign country concerned in relation to
14 that access while the vessel is in those waters.
- 15 (7) As soon as practicable after the commencement of access to data
16 held in a computer under the authority of a computer access
17 warrant in circumstances where consent to that access is required:
18 (a) in a foreign country; or
19 (b) on a vessel or aircraft that is registered under the law of a
20 foreign country;
21 the chief officer of the law enforcement agency to which the law
22 enforcement officer who applied for the warrant belongs or is
23 seconded must give the Minister evidence in writing that the access
24 has been agreed to by an appropriate consenting official of the
25 foreign country.
- 26 (8) An instrument providing evidence of the kind referred to in
27 subsection (7) is not a legislative instrument.
- 28 (9) If a vessel or aircraft that is registered under the laws of a foreign
29 country is in or above the territorial sea of another foreign country,
30 subsections (1), (2) and (3) have effect as if the reference to an
31 appropriate consenting official of the foreign country were a
32 reference to an appropriate consenting official of each foreign
33 country concerned.
- 34 (10) For the avoidance of doubt, there is no requirement for the
35 agreement of an appropriate consenting official of the foreign
36 country to the access to data held in a computer under the authority
37 of a computer access warrant of a vessel or aircraft of a foreign
-

1 country that is in Australia or in or above waters within the outer
2 limits of the territorial sea of Australia.

3 **43B Evidence obtained from extraterritorial computer access not to**
4 **be tendered in evidence unless court satisfied properly**
5 **obtained**

6 Evidence obtained from access to data held in a computer
7 undertaken in a foreign country in accordance with
8 subsection 43A(1), (2) or (3) in relation to a relevant offence
9 cannot be tendered in evidence to a court in any proceedings
10 relating to the relevant offence unless the court is satisfied that the
11 access was agreed to by an appropriate consenting official of the
12 foreign country.

13 **88 Subsection 44(1) (after paragraph (a) of the definition of**
14 **protected information)**

15 Insert:

- 16 (aa) any information (other than general computer access
17 intercept information) obtained from access to data under:
18 (i) a computer access warrant; or
19 (ii) an emergency authorisation for access to data held in a
20 computer; or

21 **90 Subsection 44(1) (at the end of subparagraph (d)(iii) of the**
22 **definition of protected information)**

23 Add “or”.

24 **91 Subsection 44(1) (after subparagraph (d)(iii) of the**
25 **definition of protected information)**

26 Insert:

- 27 (iv) in a case where the information was obtained through
28 access to data held in a computer in a foreign country,
29 or on a vessel or aircraft that is registered under the law
30 of a foreign country and that is in or above waters
31 beyond the outer limit of Australia’s territorial sea—
32 without the agreement of the appropriate consenting
33 official of that foreign country, and of any other foreign

1 country, whose agreement is required under
2 section 43A;

3 **91A Subsection 44(1) (at the end of the definition of**
4 ***protected information*)**

5 Add:

6 Note: For protection of general computer access intercept information, see
7 Part 2-6 of the *Telecommunications (Interception and Access) Act*
8 *1979*.

9 **92 Section 46 (heading)**

10 Repeal the heading, substitute:

11 **46 Dealing with records obtained by using a surveillance device or**
12 **accessing data held in a computer**

13 **93 Paragraph 46(1)(a)**

14 After “protected information”, insert “or general computer access
15 intercept information”.

16 **94 Subsection 46(2)**

17 Omit “The officer in charge of any agency that is not a law enforcement
18 agency but that, as described in subsection 45(4) or (5) or 45A(1),
19 receives records or reports obtained by use of a surveillance device:”,
20 substitute:

21 If an agency is not a law enforcement agency but, as described in
22 subsection 45(4) or (5) or 45A(1), receives records or reports
23 obtained by:

24 (aa) using a surveillance device; or

25 (ab) accessing data held in a computer;

26 the officer in charge of the agency:

27 **95 After subsection 46A(1)**

28 Insert:

29 (1A) If:

30 (a) a record or report is in the possession of a law enforcement
31 agency; and

- 1 (b) the record or report comprises information obtained from
2 access to data under a control order access warrant issued on
3 the basis of a control order made in relation to a person; and
4 (c) the warrant was issued for the purpose, or for purposes that
5 include the purpose, of obtaining information that would be
6 likely to substantially assist in connection with determining
7 whether the control order, or any succeeding control order,
8 has been, or is being, complied with; and
9 (d) access to the data occurred when the control order had been
10 made, but had not come into force because it had not been
11 served on the person; and
12 (e) the chief officer of the agency is satisfied that none of the
13 information obtained from accessing the data is likely to
14 assist in connection with:
15 (i) the protection of the public from a terrorist act; or
16 (ii) preventing the provision of support for, or the
17 facilitation of, a terrorist act; or
18 (iii) preventing the provision of support for, or the
19 facilitation of, the engagement in a hostile activity in a
20 foreign country;
21 the chief officer of the agency must cause the record or report to be
22 destroyed as soon as practicable.

23 **96 Subsection 46A(2)**

24 After “subsection (1)”, insert “or (1A)”.

25 **97 After section 47**

26 Insert:

27 **47A Protection of computer access technologies and methods**

- 28 (1) In a proceeding, a person may object to the disclosure of
29 information on the ground that the information, if disclosed, could
30 reasonably be expected to reveal details of computer access
31 technologies or methods.
32 (2) If the person conducting or presiding over the proceeding is
33 satisfied that the ground of objection is made out, the person may

- 1 order that the person who has the information not be required to
2 disclose it in the proceeding.
- 3 (3) In determining whether or not to make an order under
4 subsection (2), the person conducting or presiding over the
5 proceeding must take into account whether disclosure of the
6 information:
- 7 (a) is necessary for the fair trial of the defendant; or
8 (b) is in the public interest.
- 9 (4) Subsection (2) does not affect a provision of another law under
10 which a law enforcement officer cannot be compelled to disclose
11 information or make statements in relation to the information.
- 12 (5) If the person conducting or presiding over a proceeding is satisfied
13 that publication of any information disclosed in the proceeding
14 could reasonably be expected to reveal details of computer access
15 technologies or methods, the person must make any orders
16 prohibiting or restricting publication of the information that the
17 person considers necessary to ensure that those details are not
18 revealed.
- 19 (6) Subsection (5) does not apply to the extent that the person
20 conducting or presiding over the proceeding considers that the
21 interests of justice require otherwise.
- 22 (7) In this section:
- 23 ***computer access technologies or methods*** means:
- 24 (a) technologies or methods relating to the use of:
- 25 (i) a computer; or
26 (ii) a telecommunications facility operated or provided by
27 the Commonwealth or a carrier; or
28 (iii) any other electronic equipment; or
29 (iv) a data storage device;
30 for the purpose of obtaining access to data held in the
31 computer; or
- 32 (b) technologies or methods relating to adding, copying, deleting
33 or altering other data in a computer, if doing so is necessary
34 to achieve the purpose mentioned in paragraph (a);

1 where the technologies or methods have been, or are being,
2 deployed in giving effect to:

- 3 (c) a computer access warrant; or
4 (d) an emergency authorisation given in response to an
5 application under subsection 28(1A), 29(1A) or 30(1A).

6 *proceeding* includes a proceeding before a court, tribunal or Royal
7 Commission.

8 **98 Subsection 49(2)**

9 Omit “an authorisation referred to in paragraph (1)(b) or (c),” substitute
10 “an emergency authorisation for the use of a surveillance device, or a
11 tracking device authorisation.”

12 **99 After subsection 49(2A)**

13 Insert:

- 14 (2B) In the case of a computer access warrant, or an emergency
15 authorisation, for access to data held in a computer, the report
16 must:
- 17 (a) state whether the warrant or authorisation was executed; and
 - 18 (b) if so:
 - 19 (i) state the name of the person primarily responsible for
20 the execution of the warrant or authorisation; and
 - 21 (ii) state the name of each person involved in accessing data
22 under the warrant or authorisation; and
 - 23 (iii) state the period during which the data was accessed; and
 - 24 (iv) state the name, if known, of any person whose data was
25 accessed; and
 - 26 (v) give details of any premises at which the computer was
27 located; and
 - 28 (vi) if the warrant is issued, or the authorisation is given, in
29 respect of the investigation of a relevant offence—give
30 details of the benefit to the investigation of the accessed
31 data and of the general use made, or to be made, of any
32 evidence or information obtained by the access to data;
33 and
 - 34 (vii) if the warrant is issued, or the authorisation is given, in
35 respect of the location and safe recovery of a child to
-

- 1 whom a recovery order relates—give details of the use
2 of the accessed data in assisting with the location and
3 safe recovery of the child; and
- 4 (viii) if the warrant is issued, or the authorisation is given, for
5 the purposes of an integrity operation—give details of
6 the benefit to the operation of the accessed data and of
7 the general use made, or to be made, of any evidence or
8 information obtained by the access to data; and
- 9 (ix) if the warrant is a control order access warrant—give
10 the details specified in subsection (2C); and
- 11 (x) give details of the communication of evidence or
12 information obtained by access to data held in the
13 computer to persons other than officers of the agency;
14 and
- 15 (xi) give details of the compliance with the conditions (if
16 any) to which the warrant or authorisation was subject;
17 and
- 18 (c) if the warrant or authorisation was extended or varied, state:
19 (i) the number of extensions or variations; and
20 (ii) the reasons for them.
- 21 (2C) For the purposes of subparagraph (2B)(b)(ix), the details are:
22 (a) the benefit of obtaining access to data held in the computer
23 in:
24 (i) protecting the public from a terrorist act; or
25 (ii) preventing the provision of support for, or the
26 facilitation of, a terrorist act; or
27 (iii) preventing the provision of support for, or the
28 facilitation of, the engagement in a hostile activity in a
29 foreign country; or
30 (iv) determining whether a control order has been, or is
31 being, complied with; and
32 (b) the general use to be made of any evidence or information
33 obtained by access to data held in the computer.

34 **100 Subsection 49A(1)**

35 After “control order warrant”, insert “or control order access warrant”.

1 **101 Paragraph 49A(2)(a)**

2 After “control order warrant”, insert “or control order access warrant”.

3 **102 After paragraph 49A(2)(b)**

4 Insert:

5 (ba) subsection 27G(2), to the extent it applies to a control order
6 access warrant;

7 **103 After paragraph 49A(2)(c)**

8 Insert:

9 (ca) section 45 or subsection 46(1), to the extent it applies to
10 protected information obtained, under a control order access
11 warrant, from access to data held in a computer;

12 **104 Subsection 49A(3)**

13 After “control order warrant”, insert “or control order access warrant”.

14 **104A After section 49A**

15 Insert:

16 **49B Notification to Ombudsman in relation to concealment of access**
17 **under a computer access warrant**

18 If:

19 (a) a computer access warrant was issued in response to an
20 application made by a law enforcement officer of a law
21 enforcement agency; and

22 (b) a thing mentioned in subsection 27E(7) was done under the
23 warrant after the 28-day period mentioned in
24 paragraph 27E(7)(j);

25 the chief officer of the law enforcement agency must:

26 (c) notify the Ombudsman:

27 (i) that the warrant was issued; and

28 (ii) of the fact that the thing was done under the warrant
29 after the 28-day period mentioned in
30 paragraph 27E(7)(j); and

31 (d) do so within 7 days after the thing was done.

1 **105 Paragraphs 50(1)(g), (h) and (i)**

2 Repeal the paragraphs, substitute:

3 (g) the number of arrests made by law enforcement officers of
4 the agency during that year on the basis (wholly or partly) of
5 information obtained by:

6 (i) the use of a surveillance device under a warrant; or

7 (ii) access under a warrant to data held in a computer; or

8 (iii) an emergency authorisation for the use of a surveillance
9 device; or

10 (iv) an emergency authorisation for access to data held in a
11 computer; or

12 (v) a tracking device authorisation; and

13 (h) the number of instances during that year in which the
14 location and safe recovery of children to whom recovery
15 orders related was assisted (wholly or partly) by information
16 obtained by:

17 (i) the use of a surveillance device under a warrant; or

18 (ii) access under a warrant to data held in a computer; or

19 (iii) an emergency authorisation for the use of a surveillance
20 device; or

21 (iv) an emergency authorisation for access to data held in a
22 computer; or

23 (v) a tracking device authorisation; and

24 (i) the number of prosecutions for relevant offences that were
25 commenced during that year in which information obtained
26 by:

27 (i) the use of a surveillance device under a warrant; or

28 (ii) access under a warrant to data held in a computer; or

29 (iii) an emergency authorisation for the use of a surveillance
30 device; or

31 (iv) an emergency authorisation for access to data held in a
32 computer; or

33 (v) a tracking device authorisation;

34 was given in evidence and the number of those prosecutions
35 in which a person was found guilty; and

1 **106 Paragraph 50(1)(j)**

2 After “surveillance devices”, insert “, access to data held in computers”.

3 **107 Subsection 50A(6) (definition of *control order***
4 ***information*)**

5 Repeal the definition, substitute:

6 *control order information* means:

- 7 (a) information that, if made public, could reasonably be
8 expected to enable a reasonable person to conclude that a
9 control order warrant authorising:
10 (i) the use of a surveillance device on particular premises;
11 or
12 (ii) the use of a surveillance device in or on a particular
13 object or class of object; or
14 (iii) the use of a surveillance device in respect of the
15 conversations, activities or location of a particular
16 person;
17 is likely to be, or is not likely to be, in force; or
18 (b) information that, if made public, could reasonably be
19 expected to enable a reasonable person to conclude that a
20 control order access warrant authorising:
21 (i) access to data held in a particular computer; or
22 (ii) access to data held in a computer on particular premises;
23 or
24 (iii) access to data held in a computer associated with, used
25 by or likely to be used by, a particular person;
26 is likely to be, or is not likely to be, in force.

27 **108 Paragraph 51(b)**

28 Omit “or 27(4)”, substitute “, 27(4) or 27G(4)”.

29 **109 Paragraphs 52(1)(e), (f), (g) and (h)**

30 Repeal the paragraphs, substitute:

- 31 (e) details of each use by the agency, or by a law enforcement
32 officer of the agency, of information obtained by:
33 (i) the use of a surveillance device by a law enforcement
34 officer of the agency; or
-

- 1 (ii) access, by a law enforcement officer of the agency, to
2 data held in a computer;
- 3 (f) details of each communication by a law enforcement officer
4 of the agency to a person other than a law enforcement
5 officer of the agency of information obtained by:
- 6 (i) the use of a surveillance device by a law enforcement
7 officer of the agency; or
- 8 (ii) access, by a law enforcement officer of the agency, to
9 data held in a computer;
- 10 (g) details of each occasion when, to the knowledge of a law
11 enforcement officer of the agency, information obtained by:
- 12 (i) the use of a surveillance device by a law enforcement
13 officer of the agency; or
- 14 (ii) access, by a law enforcement officer of the agency, to
15 data held in a computer;
- 16 was given in evidence in a relevant proceeding;
- 17 (h) details of each occasion when, to the knowledge of a law
18 enforcement officer of the agency, information obtained by:
- 19 (i) the use of a surveillance device by a law enforcement
20 officer of the agency; or
- 21 (ii) access, by a law enforcement officer of the agency, to
22 data held in a computer;
- 23 was used in the location and safe recovery of a child to whom
24 a recovery order related;

25 **110 Paragraph 52(1)(j)**

26 After “subsection 46A(1)”, insert “or (1A)”.

27 **111 After subparagraph 53(2)(c)(iic)**

28 Insert:

- 29 (iiid) if the warrant is a control order access warrant that was
30 issued on the basis of a control order—the date the
31 control order was made; and

32 **111A After subsection 55(2A)**

33 Insert:

34 (2B) If:

- 1 (a) the performance of a function, or the exercise of a power,
2 conferred by Part 15 of the *Telecommunications Act 1997* is
3 in connection with a warrant; and
4 (b) a law enforcement agency has records that relate to the
5 performance of that function or the exercise of that power;
6 the Ombudsman may inspect those records in order to determine
7 the extent of compliance with Part 15 of the *Telecommunications*
8 *Act 1997* by the agency and law enforcement officers of the
9 agency.

10 **112 At the end of subsection 62(1)**

- 11 Add:
12 ; or (c) anything done by the law enforcement officer in connection
13 with:
14 (i) the communication by a person to another person; or
15 (ii) the making use of; or
16 (iii) the making of a record of; or
17 (iv) the custody of a record of;
18 information obtained from access to data under:
19 (v) a computer access warrant; or
20 (vi) an emergency authorisation for access to data held in a
21 computer.

22 **113 Subsection 62(3)**

- 23 After “section 35”, insert “or 35A”.

24 **113A Section 64**

- 25 Before “If:”, insert “(1)”.

26 **113B At the end of section 64**

- 27 Add:
28 (2) If:
29 (a) a person suffers loss or injury as a result of the use of:
30 (i) a computer; or
31 (ii) a telecommunications facility operated or provided by
32 the Commonwealth or a carrier; or
-

- 1 (iii) any other electronic equipment; or
2 (iv) a data storage device;
3 for the purpose of obtaining access to data that is held in the
4 computer; and
5 (b) the use of the computer, facility, equipment or device, as the
6 case may be, was by any of the following:
7 (i) the Australian Federal Police;
8 (ii) the Integrity Commissioner or a staff member of
9 ACLEI;
10 (iii) the Australian Crime Commission; and
11 (c) the use of the computer, facility, equipment or device, as the
12 case may be, is prohibited by the law of the State or Territory
13 in which the use occurs; and
14 (d) the use of the computer, facility, equipment or device, as the
15 case may be, is neither:
16 (i) in accordance with this Act; nor
17 (ii) in the performance of a function, or the exercise of a
18 power, conferred by a law of the Commonwealth;
19 the Commonwealth is liable to pay to the person who has suffered
20 the loss or injury:
21 (e) such compensation as is agreed on between the
22 Commonwealth and that person; or
23 (f) in default of such an agreement—such compensation as is
24 determined by action against the Commonwealth in a court of
25 a State or Territory that has jurisdiction in relation to the
26 matter.

27 **114 After section 64**

28 Insert:

29 **64A Person with knowledge of a computer or a computer system to**
30 **assist access etc.**

- 31 (1) A law enforcement officer (or another person on the officer's
32 behalf) may apply to an eligible Judge or to a nominated AAT
33 member for an order (the *assistance order*) requiring a specified
34 person to provide any information or assistance that is reasonable

- 1 and necessary to allow the law enforcement officer to do one or
2 more of the following:
- 3 (a) access data held in a computer that is the subject of:
 - 4 (i) a computer access warrant; or
 - 5 (ii) an emergency authorisation given in response to an
6 application under subsection 28(1A), 29(1A) or 30(1A);
 - 7 (b) copy data held in the computer described in paragraph (a) to
8 a data storage device;
 - 9 (c) convert into documentary form or another form intelligible to
10 a law enforcement officer:
 - 11 (i) data held in the computer described in paragraph (a); or
 - 12 (ii) data held in a data storage device to which the data was
13 copied as described in paragraph (b).

14 *Warrants and emergency authorisations relating to relevant*
15 *offences*

- 16 (2) In the case of a computer that is the subject of:
- 17 (a) a computer access warrant issued in relation to a relevant
18 offence; or
 - 19 (b) an emergency authorisation given in response to an
20 application under subsection 28(1A);
- 21 the eligible Judge or nominated AAT member may grant the
22 assistance order if the eligible Judge or nominated AAT member is
23 satisfied that:
- 24 (c) there are reasonable grounds for suspecting that access to
25 data held in the computer is necessary in the course of the
26 investigation for the purpose of enabling evidence to be
27 obtained of:
 - 28 (i) the commission of those offences; or
 - 29 (ii) the identity or location of the offenders; and
 - 30 (d) the specified person is:
 - 31 (i) reasonably suspected of having committed any of the
32 offences to which the warrant or emergency
33 authorisation relates; or
 - 34 (ii) the owner or lessee of the computer or device; or
 - 35 (iii) an employee of the owner or lessee of the computer or
36 device; or
-

- 1 (iv) a person engaged under a contract for services by the
2 owner or lessee of the computer or device; or
3 (v) a person who uses or has used the computer or device;
4 or
5 (vi) a person who is or was a system administrator for the
6 system including the computer or device; and
7 (e) the specified person has relevant knowledge of:
8 (i) the computer or device or a computer network of which
9 the computer or device forms or formed a part; or
10 (ii) measures applied to protect data held in the computer or
11 device.

12 *Warrants and emergency authorisations relating to recovery*
13 *orders*

- 14 (3) In the case of a computer that is the subject of:
15 (a) a computer access warrant issued in relation to a recovery
16 order; or
17 (b) an emergency authorisation given in response to an
18 application under subsection 29(1A);
19 the eligible Judge or nominated AAT member may grant the
20 assistance order if the eligible Judge or nominated AAT member is
21 satisfied that:
22 (c) there are reasonable grounds for suspecting that access to
23 data held in the computer may assist in the location and safe
24 recovery of the child to whom the recovery order relates; and
25 (d) the specified person is:
26 (i) the owner or lessee of the computer or
27 (ii) an employee of the owner or lessee of the computer; or
28 (iii) a person engaged under a contract for services by the
29 owner or lessee of the computer; or
30 (iv) a person who uses or has used the computer; or
31 (v) a person who is or was a system administrator for the
32 system including the computer; and
33 (e) the specified person has relevant knowledge of:
34 (i) the computer or a computer network of which the
35 computer forms or formed a part; or
36 (ii) measures applied to protect data held in the computer.
-

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36

Warrants relating to mutual assistance authorisations

- (4) In the case of a computer that is the subject of a computer access warrant issued in relation to a mutual assistance authorisation, the eligible Judge or nominated AAT member may grant the assistance order if the eligible Judge or nominated AAT member is satisfied that:
- (a) there are reasonable grounds for suspecting that access to data held in the computer is necessary, in the course of the investigation or investigative proceeding to which the authorisation relates, for the purpose of enabling evidence to be obtained of:
 - (i) the commission of the offence to which the authorisation relates; or
 - (ii) the identity or location of the persons suspected of committing the offence; and
 - (b) the specified person is:
 - (i) reasonably suspected of committing the offence to which the authorisation relates; or
 - (ii) the owner or lessee of the computer; or
 - (iii) an employee of the owner or lessee of the computer; or
 - (iv) a person engaged under a contract for services by the owner or lessee of the computer; or
 - (v) a person who uses or has used the computer; or
 - (vi) a person who is or was a system administrator for the system including the computer; and
 - (c) the specified person has relevant knowledge of:
 - (i) the computer or a computer network of which the computer forms or formed a part; or
 - (ii) measures applied to protect data held in the computer.

Warrants relating to integrity operations

- (5) In the case of a computer that is the subject of a computer access warrant issued in relation to an integrity operation, the eligible Judge or nominated AAT member may grant the assistance order if the eligible Judge or nominated AAT member is satisfied that:
- (a) there are reasonable grounds for suspecting that access to data held in the computer will assist the conduct of the

- 1 integrity operation by enabling evidence to be obtained
2 relating to the integrity, location or identity of a particular
3 staff member of the target agency; and
4 (b) the specified person is:
5 (i) the staff member; or
6 (ii) the owner or lessee of the computer; or
7 (iii) an employee of the owner or lessee of the computer; or
8 (iv) a person engaged under a contract for services by the
9 owner or lessee of the computer; or
10 (v) a person who uses or has used the computer; or
11 (vi) a person who is or was a system administrator for the
12 system including the computer; and
13 (c) the specified person has relevant knowledge of:
14 (i) the computer or a computer network of which the
15 computer forms or formed a part; or
16 (ii) measures applied to protect data held in the computer.

17 *Warrants relating to control orders*

- 18 (6) In the case of a computer that is subject to a computer access
19 warrant issued on the basis of a control order, the eligible Judge or
20 nominated AAT member may grant the assistance order if the
21 eligible Judge or nominated AAT member is satisfied that:
22 (a) there are reasonable grounds for suspecting that access to the
23 data held in the computer would be likely to substantially
24 assist in:
25 (i) protecting the public from a terrorist act; or
26 (ii) preventing the provision of support for, or the
27 facilitation of, a terrorist act; or
28 (iii) preventing the provision of support for, or the
29 facilitation of, the engagement in a hostile activity in a
30 foreign country; or
31 (iv) determining whether the control order, or any
32 succeeding control order, has been, or is being,
33 complied with; and
34 (b) the specified person is:
35 (i) the subject of the control order; or
36 (ii) the owner or lessee of the computer; or

- 1 (iii) an employee of the owner or lessee of the computer; or
2 (iv) a person engaged under a contract for services by the
3 owner or lessee of the computer; or
4 (v) a person who uses or has used the computer; or
5 (vi) a person who is or was a system administrator for the
6 system including the computer; and
7 (c) the specified person has relevant knowledge of:
8 (i) the computer or a computer network of which the
9 computer forms or formed a part; or
10 (ii) measures applied to protect data held in the computer.

11 *Emergency authorisations relating to risk of loss of evidence*

- 12 (7) In the case of a computer that is the subject of an emergency
13 authorisation given in response to an application under
14 subsection 30(1A), the eligible Judge or nominated AAT member
15 may grant the assistance order if the eligible Judge or nominated
16 AAT member is satisfied that:
17 (a) there are reasonable grounds for suspecting that access to
18 data held in the computer is necessary to prevent the loss of
19 any evidence relevant to the investigation to which the
20 subsection 30(1A) application relates; and
21 (b) the specified person is:
22 (i) reasonably suspected of having committed any of the
23 offences to which the emergency authorisation relates;
24 or
25 (ii) the owner or lessee of the computer or device; or
26 (iii) an employee of the owner or lessee of the computer or
27 device; or
28 (iv) a person engaged under a contract for services by the
29 owner or lessee of the computer or device; or
30 (v) a person who uses or has used the computer or device;
31 or
32 (vi) a person who is or was a system administrator for the
33 system including the computer or device; and
34 (c) the specified person has relevant knowledge of:
35 (i) the computer or device or a computer network of which
36 the computer or device forms or formed a part; or
-

- 1 (ii) measures applied to protect data held in the computer or
2 device.

3 *Offence*

- 4 (8) A person commits an offence if:
5 (a) the person is subject to an order under this section; and
6 (b) the person is capable of complying with a requirement in the
7 order; and
8 (c) the person omits to do an act; and
9 (d) the omission contravenes the requirement.

10 Penalty for contravention of this subsection: Imprisonment for 10
11 years or 600 penalty units, or both.

12 **115 After subsection 65(1)**

13 Insert:

14 (1A) If:

- 15 (a) information or a record is purportedly obtained through
16 accessing, under a computer access warrant or emergency
17 authorisation, particular data held in a computer; and
18 (b) there is a defect or irregularity in relation to the warrant or
19 emergency authorisation; and
20 (c) but for that defect or irregularity, the warrant or emergency
21 authorisation would be a sufficient authority for accessing the
22 data;

23 then:

- 24 (d) access to the data is taken to be as valid; and
25 (e) the information or record obtained through accessing the data
26 may be dealt with, or given in evidence in any proceeding;
27 as if the warrant or emergency authorisation did not have that
28 defect or irregularity.

29 **116 Subsection 65(2)**

30 After “subsection (1)”, insert “or (1A)”.

31 **117 After subsection 65A(2)**

32 Insert:

1 *Control order access warrant*

2 (2A) If:

3 (a) a control order access warrant was issued on the basis that an
4 interim control order was in force; and

5 (b) a court subsequently declares the interim control order to be
6 void;

7 a criminal proceeding does not lie against a person in respect of
8 anything done, or omitted to be done, in good faith by the person:

9 (c) in the purported execution of the warrant; or

10 (d) in the purported exercise of a power, or the purported
11 performance of a function or duty, in a case where the
12 purported exercise of the power, or the purported
13 performance of the function or duty, is consequential on the
14 warrant.

15 (2B) Subsection (2A) does not apply to a thing done, or omitted to be
16 done, at a particular time if, at that time, the person knew, or ought
17 reasonably to have known, of the declaration.

18 **118 Section 65B (heading)**

19 Repeal the heading, substitute:

20 **65B Dealing with information obtained under a control order**
21 **warrant, control order access warrant, tracking device**
22 **authorisation etc.—control order declared to be void**

23 **119 After subparagraph 65B(1)(a)(i)**

24 Insert:

25 (ia) a control order access warrant was issued on the basis
26 that an interim control order was in force;

27 *Telecommunications Act 1997*

28 **119A After paragraph 313(7)(c)**

29 Insert:

30 (caa) giving effect to authorisations under section 31A of that Act;
31 or

1 ***Telecommunications (Interception and Access) Act 1979***

2 **120 Subsection 5(1)**

3 Insert:

4 ***ASIO computer access intercept information*** means information
5 obtained under:

- 6 (a) an ASIO computer access warrant; or
7 (b) subsection 25A(8) of the *Australian Security Intelligence*
8 *Organisation Act 1979*; or
9 (c) subsection 27A(3C) of the *Australian Security Intelligence*
10 *Organisation Act 1979*; or
11 (d) an authorisation under section 27E of the *Australian Security*
12 *Intelligence Organisation Act 1979*; or
13 (e) subsection 27E(6) of the *Australian Security Intelligence*
14 *Organisation Act 1979*;

15 by intercepting a communication passing over a
16 telecommunications system.

17 ***ASIO computer access warrant*** means:

- 18 (a) a warrant issued under section 25A of the *Australian Security*
19 *Intelligence Organisation Act 1979*; or
20 (b) a warrant issued under section 27A of the *Australian Security*
21 *Intelligence Organisation Act 1979* that authorises the
22 Organisation to do any of the acts or things referred to in
23 subsection 25A(4) or (8) of that Act; or
24 (c) an authorisation under section 27E of the *Australian Security*
25 *Intelligence Organisation Act 1979*.

26 ***general computer access intercept information*** means information
27 obtained under a general computer access warrant by intercepting a
28 communication passing over a telecommunications system.

29 ***general computer access warrant*** means a warrant issued under
30 section 27C of the *Surveillance Devices Act 2004*.

31 ***Ombudsman official*** means:

- 32 (a) the Ombudsman; or
33 (b) a Deputy Commonwealth Ombudsman; or

1 (c) a person who is a member of the staff referred to in
2 subsection 31(1) of the *Ombudsman Act 1976*.

3 **121 Subsection 5(1) (at the end of the definition of *restricted***
4 ***record*)**

5 Add “, but does not include a record of general computer access
6 intercept information”.

7 **122 Subsection 5(1) (paragraph (b) of the definition of**
8 ***warrant*)**

9 After “definition)”, insert “, a general computer access warrant or an
10 ASIO computer access warrant”.

11 **123 After paragraph 7(2)(b)**

12 Insert:

13 (ba) the interception of a communication under subsection 25A(4)
14 or (8), 27A(1) or (3C), 27E(2) or 27E(6) of the *Australian*
15 *Security Intelligence Organisation Act 1979*; or

16 (bb) the interception of a communication under subsection 27E(7)
17 of the *Surveillance Devices Act 2004*; or

18 **123A Subsection 31(1)**

19 Omit “system by employees of the authority authorised under
20 section 31B.”, substitute:

21 system:

22 (a) if one or more carriers are specified in the request for the
23 purposes of this paragraph—by:

24 (i) employees of the security authority authorised under
25 section 31B; and

26 (ii) employees of those carriers; or

27 (b) if no carriers are specified in the request for the purposes of
28 paragraph (a)—by employees of the security authority
29 authorised under section 31B.

30 **123B Subsection 31A(1)**

31 Omit “system by employees of the security authority authorised under
32 section 31B.”, substitute:

1 system:

- 2 (a) if one or more carriers are specified in the request for the
3 purposes of paragraph 31(1)(a)—by:
4 (i) employees of the security authority authorised under
5 section 31B; and
6 (ii) employees of those carriers; or
7 (b) if no carriers are specified in the request for the purposes of
8 paragraph 31(1)(a)—by employees of the security authority
9 authorised under section 31B.

10 **123BA After subsection 31A(4)**

11 Insert:

- 12 (4A) If paragraph (1)(a) applies to the authorisation, this Part does not
13 require that an authorised interception must involve:
14 (a) one or more employees of the security authority referred to in
15 that paragraph; and
16 (b) one or more employees of a carrier referred to in that
17 paragraph;
18 acting together or in the presence of each other.

19 **123C After section 31A**

20 Insert:

21 **31AA Carrier to be notified of authorisation etc.**

- 22 (1) If:
23 (a) the Attorney-General gives a section 31A authorisation in
24 response to an application made by:
25 (i) the head (however described) of a security authority; or
26 (ii) a person acting as that head; and
27 (b) the authorisation covers the employees of a carrier;
28 the head (however described) of the security authority, or a person
29 acting as that head, must cause a copy of the authorisation to be
30 given to the authorised representative of the carrier as soon as
31 practicable.
32 (2) If:

- 1 (a) the Attorney-General has given a section 31A authorisation
2 in response to an application made by:
3 (i) the head (however described) of a security authority; or
4 (ii) a person acting as that head; and
5 (b) the authorisation is varied or revoked; and
6 (c) the authorisation covers the employees of a carrier;
7 the head (however described) of the security authority, or a person
8 acting as that head, must cause:
9 (d) an authorised representative of the carrier to be immediately
10 informed of the variation or revocation; and
11 (e) a copy of the variation or revocation to be given to the
12 authorised representative as soon as practicable.

13 **123D At the end of Part 2-4**

14 Add:

15 **31E Employees of security authorities**

- 16 (1) For the purposes of this Part:
17 (a) an ASIO employee is taken to be an employee of the
18 Organisation; and
19 (b) an ASIO affiliate is taken to be an employee of the
20 Organisation.
21 (2) For the purposes of this Part, if:
22 (a) a person is a staff member (within the meaning of the
23 *Intelligence Services Act 2001*) of an agency (within the
24 meaning of that Act); and
25 (b) the agency is a security authority;
26 the person is taken to be an employee of the security authority.

27 **124 After section 63AA**

28 Insert:

29 **63AB Dealing in general computer access intercept information etc.**

- 30 (1) A person may, for the purposes of doing a thing authorised by a
31 general computer access warrant:
-

- 1 (a) communicate general computer access intercept information
2 to another person; or
3 (b) make use of general computer access intercept information;
4 or
5 (c) make a record of general computer access intercept
6 information; or
7 (d) give general computer access intercept information in
8 evidence in a proceeding.
- 9 (2) A person may:
- 10 (a) communicate general computer access intercept information
11 to another person; or
12 (b) make use of general computer access intercept information;
13 or
14 (c) make a record of general computer access intercept
15 information;
16 if the information relates, or appears to relate, to the involvement,
17 or likely involvement, of a person in one or more of the following
18 activities:
- 19 (d) activities that present a significant risk to a person's safety;
20 (e) acting for, or on behalf of, a foreign power (within the
21 meaning of the *Australian Security Intelligence Organisation*
22 *Act 1979*);
23 (f) activities that are, or are likely to be, a threat to security;
24 (g) activities that pose a risk, or are likely to pose a risk, to the
25 operational security (within the meaning of the *Intelligence*
26 *Services Act 2001*) of the Organisation or of ASIS, AGO or
27 ASD (within the meanings of that Act);
28 (h) activities related to the proliferation of weapons of mass
29 destruction or the movement of goods listed from time to
30 time in the Defence and Strategic Goods List (within the
31 meaning of regulation 13E of the *Customs (Prohibited*
32 *Exports) Regulations 1958*);
33 (i) activities related to a contravention, or an alleged
34 contravention, by a person of a UN sanction enforcement law
35 (within the meaning of the *Charter of the United Nations Act*
36 *1945*).
- 37 (3) A person may, in connection with:
-

Schedule 2 Computer access warrants etc.

Part 1 Amendments

- 1 (a) the performance by an Ombudsman official of the
2 Ombudsman official's functions or duties; or
3 (b) the exercise by an Ombudsman official of the Ombudsman
4 official's powers;
5 communicate to the Ombudsman official, or make use of, or make
6 a record of, general computer access intercept information.
- 7 (4) An Ombudsman official may, in connection with:
8 (a) the performance by the Ombudsman official of the
9 Ombudsman official's functions or duties; or
10 (b) the exercise by the Ombudsman official of the Ombudsman
11 official's powers;
12 communicate to another person, or make use of, or make a record
13 of, general computer access intercept information.
- 14 (5) If:
15 (a) information was obtained by intercepting a communication
16 passing over a telecommunications system; and
17 (b) the interception was purportedly for the purposes of doing a
18 thing specified in a general computer access warrant; and
19 (c) the interception was not authorised by the general computer
20 access warrant;
21 then:
22 (d) a person may, in connection with:
23 (i) the performance by an Ombudsman official of the
24 Ombudsman official's functions or duties; or
25 (ii) the exercise by an Ombudsman official of the
26 Ombudsman official's powers;
27 communicate to the Ombudsman official, or make use of, or
28 make a record of, that information; and
29 (e) an Ombudsman official may, in connection with:
30 (i) the performance by the Ombudsman official of the
31 Ombudsman official's functions or duties; or
32 (ii) the exercise by the Ombudsman official of the
33 Ombudsman official's powers;
34 communicate to another person, or make use of, or make a
35 record of, that information.

- 1 (6) Despite subsection 13.3(3) of the *Criminal Code*, in a prosecution
2 for an offence against section 63 of this Act, an Ombudsman
3 official does not bear an evidential burden in relation to the matters
4 in subsection (4) or (5) of this section.

5 **63AC Dealing in ASIO computer access intercept information etc.**

- 6 (1) A person may, for the purposes of doing a thing authorised by an
7 ASIO computer access warrant:
8 (a) communicate ASIO computer access intercept information to
9 another person; or
10 (b) make use of ASIO computer access intercept information; or
11 (c) make a record of ASIO computer access intercept
12 information; or
13 (d) give ASIO computer access intercept information in evidence
14 in a proceeding.
- 15 (2) A person may:
16 (a) communicate ASIO computer access intercept information to
17 another person; or
18 (b) make use of ASIO computer access intercept information; or
19 (c) make a record of ASIO computer access intercept
20 information;
21 if the information relates, or appears to relate, to the involvement,
22 or likely involvement, of a person in one or more of the following
23 activities:
24 (d) activities that present a significant risk to a person's safety;
25 (e) acting for, or on behalf of, a foreign power (within the
26 meaning of the *Australian Security Intelligence Organisation*
27 *Act 1979*);
28 (f) activities that are, or are likely to be, a threat to security;
29 (g) activities that pose a risk, or are likely to pose a risk, to the
30 operational security (within the meaning of the *Intelligence*
31 *Services Act 2001*) of the Organisation or of ASIS, AGO or
32 ASD (within the meanings of that Act);
33 (h) activities related to the proliferation of weapons of mass
34 destruction or the movement of goods listed from time to
35 time in the Defence and Strategic Goods List (within the

- 1 meaning of regulation 13E of the *Customs (Prohibited*
2 *Exports) Regulations 1958*);
- 3 (i) activities related to a contravention, or an alleged
4 contravention, by a person of a UN sanction enforcement law
5 (within the meaning of the *Charter of the United Nations Act*
6 *1945*).
- 7 (3) A person may, in connection with:
- 8 (a) the performance by an IGIS official of the IGIS official's
9 functions or duties; or
- 10 (b) the exercise by an IGIS official of the IGIS official's powers;
11 communicate to the IGIS official, or make use of, or make a record
12 of, ASIO computer access intercept information.
- 13 (4) An IGIS official may, in connection with:
- 14 (a) the performance by the IGIS official of the IGIS official's
15 functions or duties; or
- 16 (b) the exercise by the IGIS official of the IGIS official's
17 powers;
18 communicate to another person, or make use of, or make a record
19 of, ASIO computer access intercept information.
- 20 (5) If:
- 21 (a) information was obtained by intercepting a communication
22 passing over a telecommunications system; and
- 23 (b) the interception was purportedly for the purposes of doing a
24 thing specified in an ASIO computer access warrant; and
- 25 (c) the interception was not authorised by the ASIO computer
26 access warrant;
- 27 then:
- 28 (d) a person may, in connection with:
- 29 (i) the performance by an IGIS official of the IGIS
30 official's functions or duties; or
- 31 (ii) the exercise by an IGIS official of the IGIS official's
32 powers;
33 communicate to the IGIS official, or make use of, or make a
34 record of, that information; and
- 35 (e) an IGIS official may, in connection with:
-

- 1 (i) the performance by the IGIS official of the IGIS
2 official's functions or duties; or
3 (ii) the exercise by the IGIS official of the IGIS official's
4 powers;
5 communicate to another person, or make use of, or make a
6 record of, that information.
- 7 (6) Despite subsection 13.3(3) of the *Criminal Code*, in a prosecution
8 for an offence against section 63 of this Act, an IGIS official does
9 not bear an evidential burden in relation to the matters in
10 subsection (4) or (5) of this section.

11 **124A At the end of section 63B**

12 Add:

- 13 (5) If an employee of a carrier has obtained lawfully intercepted
14 information under a section 31A authorisation that was given in
15 response to an application made by the head (however described)
16 of a security authority or a person acting as that head, the employee
17 may:
18 (a) communicate the information to:
19 (i) an employee of the security authority; or
20 (ii) another employee of the carrier; or
21 (iii) if the authorisation covers the employees of one or more
22 other carriers—an employee of any of those other
23 carriers; or
24 (b) make use of the information; or
25 (c) make a record of the information;
26 if:
27 (d) the employee does so for the purposes of the development or
28 testing of technologies, or interception capabilities, to which
29 the authorisation relates; and
30 (e) the communication or use of the information, or the making
31 of the record, as the case may be, does not contravene a
32 condition to which the authorisation is subject.

33 **125 Paragraph 64(1)(a)**

34 After "foreign intelligence information", insert "or ASIO computer
35 access intercept information".

1 **126 Paragraph 65(1)(a)**

2 After “information”, insert “other than ASIO computer access intercept
3 information”.

4 **126AA At the end of section 65 (after the note)**

5 Add:

6 (4) If lawfully intercepted information was obtained under a
7 section 31A authorisation, subsection (1) of this section does not
8 authorise the communication of the information in accordance with
9 subsection 18(3) of the *Australian Security Intelligence*
10 *Organisation Act 1979* to:

11 (a) a staff member of an authority of the Commonwealth; or

12 (b) a staff member of an authority of a State;

13 unless the communication is for the purpose of the development or
14 testing of technologies, or interception capabilities, of:

15 (c) that authority; or

16 (d) the Organisation.

17 (5) If lawfully intercepted information was obtained under a
18 section 31A authorisation, subsection (1) of this section does not
19 authorise the communication of the information in accordance with
20 subsection 18(4A) of the *Australian Security Intelligence*
21 *Organisation Act 1979* to a staff member of ASIS, ASD or AGO
22 unless the communication is for the purpose of the development or
23 testing of technologies, or interception capabilities, of:

24 (a) ASIS, ASD or AGO, as the case requires; or

25 (b) the Organisation.

26 (6) If lawfully intercepted information was obtained under a
27 section 31A authorisation, subsection (1) of this section does not
28 authorise the communication of the information in accordance with
29 subsection 19A(4) of the *Australian Security Intelligence*
30 *Organisation Act 1979* to a staff member of a body referred to in
31 paragraph 19A(1)(d) or (e) of that Act unless the communication is
32 for the purpose of the development or testing of technologies, or
33 interception capabilities, of:

34 (a) that body; or

35 (b) the Organisation.

1 (7) For the purposes of subsections (4), (5) and (6), *authority of the*
2 *Commonwealth, authority of a State, ASIS, ASD, AGO* and *staff*
3 *member* have the same respective meanings as in the *Australian*
4 *Security Intelligence Organisation Act 1979*.

5 **126A Paragraph 65A(1)(a)**

6 After “foreign intelligence information”, insert “or information obtained
7 under a section 31A authorisation”.

8 **127 Paragraph 67(1)(a)**

9 After “foreign intelligence information”, insert “or general computer
10 access intercept information”.

11 **128 Section 68**

12 After “communicate lawfully intercepted information”, insert “(other
13 than general computer access intercept information)”.

14 **129 Subsection 74(1)**

15 After “foreign intelligence information”, insert “, general computer
16 access intercept information or ASIO computer access intercept
17 information”.

18 **130 Subsection 75(1)**

19 After “other than”, insert “a general computer access warrant or”.

20 **131 Paragraphs 77(1)(a) and (b)**

21 After “63A,”, insert “63AB, 63AC,”.

22 **131A After paragraph 108(2)(ca)**

23 Insert:

24 (cb) accessing a stored communication under a general computer
25 access warrant; or

1 **Part 2—Application provisions**

2 **132 Application—computer access warrants**

- 3 (1) The amendments of sections 25A and 27A of the *Australian Security*
4 *Intelligence Organisation Act 1979* made by this Schedule apply in
5 relation to a warrant issued after the commencement of this item.
- 6 (2) The amendments of section 27E of the *Australian Security Intelligence*
7 *Organisation Act 1979* made by this Schedule apply in relation to an
8 authorisation given after the commencement of this item.
- 9 (3) The amendments of sections 50 and 50A of the *Surveillance Devices*
10 *Act 2004* made by this Schedule apply in relation to a report in respect
11 of:
12 (a) the financial year in which this item commences; or
13 (b) a later financial year.
- 14 (4) The amendment of section 31 of the *Telecommunications (Interception*
15 *and Access) Act 1979* made by this Schedule applies in relation to a
16 request made after the commencement of this item.
- 17 (5) The amendments of section 31A of the *Telecommunications*
18 *(Interception and Access) Act 1979* made by this Schedule apply in
19 relation to an authorisation given in response to a request made after the
20 commencement of this item.

1 **Part 3—Amendments contingent on the**
2 **commencement of the Crimes Legislation**
3 **Amendment (International Crime**
4 **Cooperation and Other Measures) Act 2018**

5 *International Criminal Court Act 2002*

6 **133 After Division 12A of Part 4**

7 Insert:

8 **Division 12B—Requests for access to data held in**
9 **computers**

10 **79B Authorising applications for computer access warrants**

- 11 (1) The Attorney-General may authorise, in writing, an eligible law
12 enforcement officer to apply for a computer access warrant under
13 section 27A of the *Surveillance Devices Act 2004* if:
- 14 (a) the ICC has requested the Attorney-General to arrange for the
15 access to data held in a computer (the *target computer*); and
 - 16 (b) the Attorney-General is satisfied that an investigation is
17 being conducted by the Prosecutor, or a proceeding is before
18 the ICC; and
 - 19 (c) the Attorney-General is satisfied that the ICC has given
20 appropriate undertakings for:
 - 21 (i) ensuring that data obtained as a result of access under
22 the warrant will only be used for the purpose for which
23 it is communicated to the ICC; and
 - 24 (ii) the destruction of a document or other thing containing
25 data obtained as a result of access under the warrant;
26 and
 - 27 (iii) any other matter the Attorney-General considers
28 appropriate.

29 Note: The eligible law enforcement officer can only apply for the warrant if
30 the officer reasonably suspects that the access to data held in the target

Schedule 2 Computer access warrants etc.

Part 3 Amendments contingent on the commencement of the Crimes Legislation Amendment (International Crime Cooperation and Other Measures) Act 2018

- 1 computer is necessary for the investigation or proceeding (see
2 subsection 27A(4) of the *Surveillance Devices Act 2004*).
- 3 (2) The target computer may be any one or more of the following:
4 (a) a particular computer;
5 (b) a computer on particular premises;
6 (c) a computer associated with, used by or likely to be used by, a
7 person (whose identity may or may not be known).
- 8 (3) In this section:
- 9 **computer** has the same meaning as in the *Surveillance Devices Act*
10 *2004*.
- 11 **data** has the same meaning as in the *Surveillance Devices Act*
12 *2004*.
- 13 **data held in a computer** has the same meaning as in the
14 *Surveillance Devices Act 2004*.
- 15 **eligible law enforcement officer** means a person mentioned in
16 column 3 of table item 5 in subsection 6A(6), or column 3 of table
17 item 5 in subsection 6A(7), of the *Surveillance Devices Act 2004*.

18 ***International War Crimes Tribunals Act 1995***

19 **134 After Division 1A of Part 4**

20 Insert:

21 **Division 1B—Requests for access to data held in computers**

22 **32B Authorising applications for computer access warrants**

- 23 (1) The Attorney-General may authorise, in writing, an eligible law
24 enforcement officer to apply for a computer access warrant under
25 section 27A of the *Surveillance Devices Act 2004* if:
26 (a) a Tribunal has requested the Attorney-General to arrange for
27 access to data held in a computer (the **target computer**); and
28 (b) the Attorney-General is satisfied that a proceeding is before,
29 or an investigation is being conducted by, the Tribunal; and

- 1 (c) the Attorney-General is satisfied that the Tribunal has given
2 appropriate undertakings for:
3 (i) ensuring that data obtained as a result of the access
4 under the warrant will only be used for the purpose for
5 which it is communicated to the Tribunal; and
6 (ii) the destruction of a document or other thing containing
7 data obtained as a result of access under the warrant;
8 and
9 (iii) any other matter the Attorney-General considers
10 appropriate.

11 Note: The eligible law enforcement officer can only apply for the warrant if
12 the officer reasonably suspects that the access to data held in the target
13 computer is necessary for the investigation or proceeding (see
14 subsection 27A(4) of the *Surveillance Devices Act 2004*).

15 (2) In this section:

16 ***computer*** has the same meaning as in the *Surveillance Devices Act*
17 *2004*.

18 ***data*** has the same meaning as in the *Surveillance Devices Act*
19 *2004*.

20 ***data held in a computer*** has the same meaning as in the
21 *Surveillance Devices Act 2004*.

22 ***eligible law enforcement officer*** means a person mentioned in
23 column 3 of table item 5 in subsection 6A(6), or column 3 of table
24 item 5 in subsection 6A(7), of the *Surveillance Devices Act 2004*.

25 ***Surveillance Devices Act 2004***

26 **135 Subsection 6(1) (definition of *international assistance*** 27 ***application*)**

28 Repeal the definition, substitute:

29 ***international assistance application*** means:

- 30 (a) an application for a surveillance device warrant; or
31 (b) an application for a computer access warrant;
32 made under an international assistance authorisation.

1 **136 Subsection 6(1) (paragraph (a) of the definition of**
2 ***international assistance authorisation*)**

3 After “15CA(1)”, insert “or 15CC(1)”.

4 **137 Subsection 27A(4)**

5 Repeal the subsection, substitute:

6 *Warrants sought for international assistance investigations*

7 (4) A law enforcement officer (or a person on the officer’s behalf) may
8 apply for the issue of a computer access warrant if the officer:

9 (a) is authorised to do so under an international assistance
10 authorisation; and

11 (b) suspects on reasonable grounds that access to data held in a
12 computer (the *target computer*) is necessary, in the course of
13 the investigation or investigative proceeding to which the
14 authorisation relates, for the purpose of enabling evidence to
15 be obtained of:

16 (i) the commission of an offence to which the authorisation
17 relates; or

18 (ii) the identity or location of the persons suspected of
19 committing the offence.

20 **138 Paragraphs 27C(1)(c) and (2)(a)**

21 Omit “a mutual assistance authorisation”, substitute “an international
22 assistance authorisation”.

23 **139 Paragraph 27C(2)(f)**

24 Repeal the paragraph, substitute:

25 (f) in the case of a warrant sought in relation to an international
26 assistance authorisation—the likely evidentiary or
27 intelligence value of any evidence or information sought to
28 be obtained, to the extent that this is possible to determine
29 from information obtained from the international entity to
30 which the authorisation relates; and

31 **140 Subparagraph 27D(1)(b)(iv)**

32 Repeal the paragraph, substitute:

1 (iv) if the warrant relates to an international assistance
2 authorisation—each offence to which the authorisation
3 relates; and

4 **141 Paragraph 27E(3)(c)**

5 Omit “a mutual assistance authorisation”, substitute “an international
6 assistance authorisation”.

7 **142 Paragraph 27H(4)(a)**

8 Omit “a mutual assistance authorisation”, substitute “an international
9 assistance authorisation”.

10 **143 Subparagraph 27H(4)(b)(i)**

11 Repeal the subparagraph, substitute:

12 (i) the commission of any offence to which the
13 authorisation relates; or

14 **144 Paragraph 27H(9)(c)**

15 Repeal the paragraph, substitute:

16 (c) if the warrant was issued in relation to an international
17 assistance authorisation—of enabling evidence to be obtained
18 of:

19 (i) the commission of any offence to which the
20 authorisation relates; or

21 (ii) the identity or location of the persons suspected of
22 committing the offence;

23 **145 Subsection 64A(4)**

24 Repeal the subsection, substitute:

25 *Warrants relating to international assistance authorisations*

26 (4) In the case of a computer that is the subject of a computer access
27 warrant issued in relation to an international assistance
28 authorisation, the eligible Judge or nominated AAT member may
29 grant the assistance order if the eligible Judge or nominated AAT
30 member is satisfied that:

Schedule 2 Computer access warrants etc.

Part 3 Amendments contingent on the commencement of the Crimes Legislation
Amendment (International Crime Cooperation and Other Measures) Act 2018

- 1 (a) there are reasonable grounds for suspecting that access to
2 data held in the computer is necessary, in the course of the
3 investigation or investigative proceeding to which the
4 authorisation relates, for the purpose of enabling evidence to
5 be obtained of:
- 6 (i) the commission of an offence to which the authorisation
7 relates; or
8 (ii) the identity or location of the persons suspected of
9 committing the offence; and
- 10 (b) the specified person is:
- 11 (i) reasonably suspected of committing an offence to which
12 the authorisation relates; or
13 (ii) the owner or lessee of the computer; or
14 (iii) an employee of the owner or lessee of the computer; or
15 (iv) a person engaged under a contract for services by the
16 owner or lessee of the computer; or
17 (v) a person who uses or has used the computer; or
18 (vi) a person who is or was a system administrator for the
19 system including the computer; and
- 20 (c) the specified person has relevant knowledge of:
- 21 (i) the computer or a computer network of which the
22 computer forms or formed a part; or
23 (ii) measures applied to protect data held in the computer.

24 **146 Application of amendments**

25 The amendments made by this Part apply in relation to a request made
26 to the Attorney-General by the ICC, a Tribunal or a foreign country:

- 27 (a) at or after the commencement of this item; or
28 (b) before the commencement of this item, if, immediately
29 before that commencement, the Attorney-General had yet to
30 make a decision on the request;

31 whether conduct, a crime or an offence to which the request relates
32 occurred before, on or after that commencement.

1 **Schedule 3—Search warrants issued under**
2 **the Crimes Act 1914**
3

4 ***Crimes Act 1914***

5 **1 Subsection 3C(1)**

6 Insert:

7 ***account-based data*** has the meaning given by section 3CAA.

8 ***carrier*** means:

9 (a) a carrier within the meaning of the *Telecommunications Act*
10 *1997*; or

11 (b) a carriage service provider within the meaning of that Act.

12 ***communication in transit*** means a communication (within the
13 meaning of the *Telecommunications Act 1997*) passing over a
14 telecommunications network (within the meaning of that Act).

15 ***electronic service*** has the same meaning as in the *Enhancing*
16 *Online Safety Act 2015*.

17 ***telecommunications facility*** means a facility within the meaning of
18 the *Telecommunications Act 1997*.

19 **2 After section 3C**

20 Insert:

21 **3CAA Account-based data**

22 (1) For the purposes of this Part, if:

23 (a) an electronic service has accounts for end-users; and

24 (b) either:

25 (i) a person holds an account with the electronic service; or

26 (ii) a person is, or is likely to be, a user of an account with
27 the electronic service; and

28 (c) the person can (with the use of appropriate equipment) access
29 particular data provided by the service;

- 1 the data is *account-based data* in relation to the person.
- 2 (2) For the purposes of this Part, if:
- 3 (a) an electronic service has accounts for end-users; and
- 4 (b) either:
- 5 (i) a deceased person held, before the person's death, an
- 6 account with the electronic service; or
- 7 (ii) a deceased person, before the person's death, was, or
- 8 was likely to be, a user of an account with the electronic
- 9 service; and
- 10 (c) the deceased person could, before the person's death (with
- 11 the use of appropriate equipment), access particular data
- 12 provided by the service;
- 13 the data is *account-based data* in relation to the deceased person.
- 14 (3) For the purposes of this section, *account* has the same meaning as
- 15 in the *Enhancing Online Safety Act 2015*.

16 3 After subsection 3F(2)

17 Insert:

- 18 (2A) A warrant that is in force authorises the executing officer or a
- 19 constable assisting:
- 20 (a) to use:
- 21 (i) a computer, or data storage device, found in the course
- 22 of a search authorised under the warrant; or
- 23 (ii) a telecommunications facility operated or provided by
- 24 the Commonwealth or a carrier; or
- 25 (iii) any other electronic equipment; or
- 26 (iv) a data storage device;
- 27 for the purpose of obtaining access to data (the *relevant data*)
- 28 that is held in the computer or device mentioned in
- 29 subparagraph (i) at any time when the warrant is in force, in
- 30 order to determine whether the relevant data is evidential
- 31 material of a kind specified in the warrant; and
- 32 (b) if necessary to achieve the purpose mentioned in
- 33 paragraph (a)—to add, copy, delete or alter other data in the
- 34 computer or device mentioned in subparagraph (a)(i); and

- 1 (c) if, having regard to other methods (if any) of obtaining access
 2 to the relevant data which are likely to be as effective, it is
 3 reasonable in all the circumstances to do so:
 4 (i) to use any other computer or a communication in transit
 5 to access the relevant data; and
 6 (ii) if necessary to achieve that purpose—to add, copy,
 7 delete or alter other data in the computer or the
 8 communication in transit; and
 9 (d) to copy any data to which access has been obtained, and that:
 10 (i) appears to be relevant for the purposes of determining
 11 whether the relevant data is evidential material of a kind
 12 specified in the warrant; or
 13 (ii) is evidential material of a kind specified in the warrant;
 14 and
 15 (e) to do any other thing reasonably incidental to any of the
 16 above.

17 Note: As a result of the warrant, a person who, by means of a
 18 telecommunications facility, obtains access to data stored in a
 19 computer etc. will not commit an offence under Part 10.7 of the
 20 *Criminal Code* or equivalent State or Territory laws (provided that the
 21 person acts within the authority of the warrant).

22 (2B) A warrant that is in force authorises the executing officer or a
 23 constable assisting:

- 24 (a) to use:
 25 (i) a computer found in the course of a search authorised
 26 under the warrant; or
 27 (ii) a telecommunications facility operated or provided by
 28 the Commonwealth or a carrier; or
 29 (iii) any other electronic equipment;
 30 for the purpose of obtaining access to data (the **relevant**
 31 **account-based data**) that is account-based data in relation to:
 32 (iv) a person who is the owner or lessee of the computer
 33 mentioned in subparagraph (i); or
 34 (v) a person who uses or has used the computer mentioned
 35 in subparagraph (i); or
 36 (vi) a deceased person who, before the person's death, was
 37 the owner or lessee of the computer mentioned in
 38 subparagraph (i); or

- 1 (vii) a deceased person who, before the person's death, used
2 the computer mentioned in subparagraph (i);
3 in order to determine whether the relevant account-based data
4 is evidential material of a kind specified in the warrant; and
5 (b) if necessary to achieve the purpose mentioned in
6 paragraph (a)—to add, copy, delete or alter other data in the
7 computer mentioned in subparagraph (a)(i); and
8 (c) if, having regard to other methods (if any) of obtaining access
9 to the relevant account-based data which are likely to be as
10 effective, it is reasonable in all the circumstances to do so:
11 (i) to use any other computer or a communication in transit
12 to access the relevant account-based data; and
13 (ii) if necessary to achieve that purpose—to add, copy,
14 delete or alter other data in the computer or the
15 communication in transit; and
16 (d) to copy any data to which access has been obtained, and that:
17 (i) appears to be relevant for the purposes of determining
18 whether the relevant account-based data is evidential
19 material of a kind specified in the warrant; or
20 (ii) is evidential material of a kind specified in the warrant;
21 and
22 (e) to do any other thing reasonably incidental to any of the
23 above.
- 24 (2C) Subsections (2A) and (2B) do not authorise the addition, deletion
25 or alteration of data, or the doing of any thing, that is likely to:
26 (a) materially interfere with, interrupt or obstruct:
27 (i) a communication in transit; or
28 (ii) the lawful use by other persons of a computer;
29 unless the addition, deletion or alteration, or the doing of the
30 thing, is necessary to do one or more of the things specified
31 in the warrant; or
32 (b) cause any other material loss or damage to other persons
33 lawfully using a computer.
- 34 (2D) In the case of a warrant that is in force in relation to premises, it is
35 immaterial whether a thing mentioned in subsection (2A) or (2B) is
36 done:
37 (a) at the premises; or
-

1 (b) at any other place.

2 (2E) In the case of a warrant that is in force in relation to a person, it is
3 immaterial whether a thing mentioned in subsection (2A) or (2B) is
4 done:

- 5 (a) in the presence of the person; or
6 (b) at any other place.

7 **4 Subsection 3K(3A)**

8 Omit “14 days.”, substitute:

9 whichever of the following is applicable:

- 10 (a) if the thing is a computer or data storage device—30 days;
11 (b) otherwise—14 days.

12 **5 Subsection 3K(3B)**

13 Omit “14 days”, substitute “the time applicable under subsection (3A)”.

14 **6 Subsection 3K(3D)**

15 Omit “7 days.”, substitute:

16 whichever of the following is applicable:

- 17 (a) if the thing is a computer or data storage device—14 days;
18 (b) otherwise—7 days.

19 **6A At the end of section 3K**

20 Add:

21 *Extended powers of examination and processing*

22 (5) For the purposes of this section, if a computer or data storage
23 device (the *relevant computer or device*) was found in the course
24 of a search authorised under a warrant, the examination or
25 processing of the relevant computer or device may include:

- 26 (a) using:
27 (i) the relevant computer or device; or
28 (ii) a telecommunications facility operated or provided by
29 the Commonwealth or a carrier; or
30 (iii) any other electronic equipment; or
-

- 1 (iv) a data storage device;
2 for the purpose of obtaining access to data (the *relevant data*)
3 that is held in the relevant computer or device in order to
4 determine whether the relevant computer or device is a thing
5 that may be seized under the warrant; and
6 (b) if necessary to achieve the purpose mentioned in
7 paragraph (a)—to add, copy, delete or alter other data in the
8 relevant computer or device; and
9 (c) if, having regard to other methods (if any) of obtaining access
10 to the relevant data which are likely to be as effective, it is
11 reasonable in all the circumstances to do so:
12 (i) to use any other computer or a communication in transit
13 to access the relevant data; and
14 (ii) if necessary to achieve that purpose—to add, copy,
15 delete or alter other data in the computer or the
16 communication in transit; and
17 (d) to copy any data to which access has been obtained, and that
18 appears to be relevant for the purposes of determining
19 whether the relevant computer or device is a thing that may
20 be seized under the warrant; and
21 (e) to do any other thing reasonably incidental to any of the
22 above.
- 23 (6) For the purposes of this section, if a computer (the *relevant*
24 *computer*) was found in the course of a search authorised under a
25 warrant, the examination or processing of the relevant computer
26 may include:
27 (a) using:
28 (i) the relevant computer; or
29 (ii) a telecommunications facility operated or provided by
30 the Commonwealth or a carrier; or
31 (iii) any other electronic equipment;
32 for the purpose of obtaining access to data (the *relevant*
33 *account-based data*) that is account-based data in relation to:
34 (iv) a person who is the owner or lessee of the relevant
35 computer; or
36 (v) a person who uses or has used the relevant computer; or

- 1 (vi) a deceased person who, before the person's death, was
2 the owner or lessee of the relevant computer; or
3 (vii) a deceased person who, before the person's death, used
4 the relevant computer;
5 in order to determine whether the relevant computer is a
6 thing that may be seized under the warrant; and
7 (b) if necessary to achieve the purpose mentioned in
8 paragraph (a)—to add, copy, delete or alter other data in the
9 relevant computer; and
10 (c) if, having regard to other methods (if any) of obtaining access
11 to the relevant account-based data which are likely to be as
12 effective, it is reasonable in all the circumstances to do so:
13 (i) to use any other computer or a communication in transit
14 to access the relevant account-based data; and
15 (ii) if necessary to achieve that purpose—to add, copy,
16 delete or alter other data in the computer or the
17 communication in transit; and
18 (d) to copy any data to which access has been obtained, and that
19 appears to be relevant for the purposes of determining
20 whether the relevant computer is a thing that may be seized
21 under the warrant; and
22 (e) to do any other thing reasonably incidental to any of the
23 above.
- 24 (7) Subsections (5) and (6) do not authorise the addition, deletion or
25 alteration of data, or the doing of any thing, that is likely to:
26 (a) materially interfere with, interrupt or obstruct:
27 (i) a communication in transit; or
28 (ii) the lawful use by other persons of a computer;
29 unless the addition, deletion or alteration, or the doing of the
30 thing, is necessary to determine:
31 (iii) in the case of subsection (5)—whether the relevant
32 computer or device is a thing that may be seized under
33 the warrant referred to in that subsection; or
34 (iv) in the case of subsection (6)—whether the relevant
35 computer is a thing that may be seized under the warrant
36 referred to in that subsection; or

1 (b) cause any other material loss or damage to other persons
2 lawfully using a computer.

3 (8) In the case of a warrant that was in force in relation to premises, it
4 is immaterial whether a thing mentioned in subsection (5) or (6) is
5 done:

6 (a) at the premises; or

7 (b) at any other place.

8 (9) In the case of a warrant that was in force in relation to a person, it
9 is immaterial whether a thing mentioned in subsection (5) or (6) is
10 done:

11 (a) in the presence of the person; or

12 (b) at any other place.

13 **7 Subsection 3LAA(1)**

14 Omit “to access data (including data held at another place).”, substitute:
15 to:

16 (a) access data (including data held at another place); or

17 (b) access account-based data.

18 **8 After subparagraph 3LA(1)(a)(i)**

19 Insert:

20 (ia) is found in the course of an ordinary search of a person,
21 or a frisk search of a person, authorised by a warrant
22 under section 3E; or

23 **9 Subsection 3LA(5)**

24 Repeal the subsection, substitute:

25 *Offences*

26 (5) A person commits an offence if:

27 (a) the person is subject to an order under this section; and

28 (b) the person is capable of complying with a requirement in the
29 order; and

30 (c) the person omits to do an act; and

31 (d) the omission contravenes the requirement.

1 Penalty: Imprisonment for 5 years or 300 penalty units, or both.

2 (6) A person commits an offence if:

- 3 (a) the person is subject to an order under this section; and
4 (b) the person is capable of complying with a requirement in the
5 order; and
6 (c) the person omits to do an act; and
7 (d) the omission contravenes the requirement; and
8 (e) the offence to which the relevant warrant relates is:
9 (i) a serious offence; or
10 (ii) a serious terrorism offence.

11 Penalty for contravention of this subsection: Imprisonment for 10
12 years or 600 penalty units, or both.

13 **10 After paragraph 3N(2)(a)**

14 Insert:

- 15 (aa) the thing embodies data that was accessed under the warrant
16 at a place other than the premises; or

17 **10A At the end of Division 2 of Part IAA**

18 Add:

19 **3SA Relationship of this Division to parliamentary privileges and**
20 **immunities**

21 To avoid doubt, this Division does not affect the law relating to the
22 powers, privileges and immunities of any of the following:

- 23 (a) each House of the Parliament;
24 (b) the members of each House of the Parliament;
25 (c) the committees of each House of the Parliament and joint
26 committees of both Houses of the Parliament.

27 **11 After subsection 3ZQV(3)**

28 Insert:

- 29 (3A) If the electronic equipment was seized under a warrant,
30 subsection (2) does not apply to data that was generated after the
31 expiry of the warrant.

1 **12 Application of amendments**

2 The amendments of sections 3F, 3K, 3LAA, 3LA, 3N and 3ZQV of the
3 *Crimes Act 1914* made by this Schedule apply in relation to a warrant
4 issued after the commencement of this item.

1 **Schedule 4—Search warrants issued under**
2 **the Customs Act 1901**
3

4 ***Customs Act 1901***

5 **1 Subsection 183UA(1)**

6 Insert:

7 *communication in transit* means a communication (within the
8 meaning of the *Telecommunications Act 1997*) passing over a
9 telecommunications network (within the meaning of that Act).

10 *recently used conveyance*, in relation to a search of a person,
11 means a conveyance that the person had operated or occupied at
12 any time within 24 hours before the search commenced.

13 **1A Subsection 183UA(1) (definition of search warrant)**

14 After “section 198”, insert “or 199A”.

15 **2 Subsection 183UA(1)**

16 Insert:

17 *serious offence* has the same meaning as in Part IAA of the *Crimes*
18 *Act 1914*.

19 *telecommunications facility* means a facility within the meaning of
20 the *Telecommunications Act 1997*.

21 **3 Section 198 (heading)**

22 Repeal the heading, substitute:

23 **198 When search warrants relating to premises can be issued**

24 **4 Section 199 (heading)**

25 Repeal the heading, substitute:

1 **199 The things that are authorised by a search warrant relating to**
2 **premises**

3 **4A After subsection 199(4)**

4 Insert:

5 (4A) A warrant that is in force in relation to premises authorises the
6 executing officer or a person assisting:

7 (a) to use:

8 (i) a computer, or data storage device, found in the course
9 of a search authorised under the warrant; or

10 (ii) a telecommunications facility operated or provided by
11 the Commonwealth or a carrier; or

12 (iii) any other electronic equipment; or

13 (iv) a data storage device;

14 for the purpose of obtaining access to data (the *relevant data*)
15 that is held in the computer or device mentioned in
16 subparagraph (i) at any time when the warrant is in force, in
17 order to determine whether the relevant data is evidential
18 material of a kind specified in the warrant; and

19 (b) if necessary to achieve the purpose mentioned in
20 paragraph (a)—to add, copy, delete or alter other data in the
21 computer or device mentioned in subparagraph (a)(i); and

22 (c) if, having regard to other methods (if any) of obtaining access
23 to the relevant data which are likely to be as effective, it is
24 reasonable in all the circumstances to do so:

25 (i) to use any other computer or a communication in transit
26 to access the relevant data; and

27 (ii) if necessary to achieve that purpose—to add, copy,
28 delete or alter other data in the computer or the
29 communication in transit; and

30 (d) to copy any data to which access has been obtained, and that:

31 (i) appears to be relevant for the purposes of determining
32 whether the relevant data is evidential material of a kind
33 specified in the warrant; or

34 (ii) is evidential material of a kind specified in the warrant;
35 and

1 (e) to do any other thing reasonably incidental to any of the
2 above.

3 Note: As a result of the warrant, a person who, by means of a
4 telecommunications facility, obtains access to data stored in a
5 computer etc. will not commit an offence under Part 10.7 of the
6 *Criminal Code* or equivalent State or Territory laws (provided that the
7 person acts within the authority of the warrant).

8 (4B) Subsection (4A) does not authorise the addition, deletion or
9 alteration of data, or the doing of any thing, that is likely to:

10 (a) materially interfere with, interrupt or obstruct:

11 (i) a communication in transit; or

12 (ii) the lawful use by other persons of a computer;

13 unless the addition, deletion or alteration, or the doing of the
14 thing, is necessary to do one or more of the things specified
15 in the warrant; or

16 (b) cause any other material loss or damage to other persons
17 lawfully using a computer.

18 (4C) It is immaterial whether a thing mentioned in subsection (4A) is
19 done:

20 (a) at the warrant premises; or

21 (b) at any other place.

22 **5 After section 199**

23 Insert:

24 **199A When search warrants relating to persons can be issued**

25 (1) A judicial officer may issue a warrant authorising an ordinary
26 search or a frisk search of a person if the judicial officer is
27 satisfied, by information on oath or affirmation, that there are
28 reasonable grounds for suspecting that the person has in the
29 person's possession, or will within the next 72 hours have in the
30 person's possession, any computer, or data storage device, that is
31 evidential material.

32 (2) If the person applying for the warrant has, at any time previously,
33 applied for a warrant under this section relating to the same person,

- 1 the person applying for the warrant must state particulars of those
2 applications, and their outcome, in the information.
- 3 (3) If a judicial officer issues a warrant, the judicial officer is to state
4 in the warrant:
- 5 (a) the offence to which the warrant relates; and
 - 6 (b) the name or description of the person to whom the warrant
7 relates; and
 - 8 (c) the name of the authorised person who, unless the authorised
9 person inserts the name of another authorised person in the
10 warrant, is to be responsible for executing the warrant; and
 - 11 (d) the time at which the warrant expires (see subsection (4));
12 and
 - 13 (e) whether the warrant may be executed at any time or only
14 during particular hours.
- 15 (4) The time stated in the warrant under paragraph (3)(d) as the time at
16 which the warrant expires must be a time that is not later than the
17 end of the seventh day after the day on which the warrant is issued.
- 18 Example: If a warrant is issued at 3 pm on a Monday, the expiry time specified
19 must not be later than midnight on Monday in the following week.
- 20 (5) The judicial officer is also to state, in a warrant in relation to a
21 person:
- 22 (a) that the warrant authorises the seizure of a computer or data
23 storage device found, in the course of the search, on or in the
24 possession of the person or in a recently used conveyance, if
25 the executing officer or a person assisting believes on
26 reasonable grounds that:
 - 27 (i) the computer or device is evidential material in relation
28 to an offence to which the warrant relates; and
 - 29 (ii) the seizure of the computer or device is necessary to
30 prevent its concealment, loss or destruction or its use in
31 committing an offence; and
 - 32 (b) the kind of search of a person that the warrant authorises.
- 33 (6) Paragraph (3)(d) and subsection (4) do not prevent the issue of
34 successive warrants in relation to the same person.

1 **199B The things that are authorised by a search warrant relating to**
2 **a person**

3 (1) A warrant that is in force in relation to a person (the *target person*)
4 authorises the executing officer or person assisting:

5 (a) to search:

6 (i) the target person as specified in the warrant; and

7 (ii) any recently used conveyance;

8 for computers or data storage devices of the kind specified in
9 the warrant; and

10 (b) to:

11 (i) seize computers or data storage devices of that kind; or

12 (ii) record fingerprints from computers or data storage
13 devices; or

14 (iii) to take samples for forensic purposes from computers or
15 data storage devices;

16 found in the course of the search; and

17 (c) to seize other things found on or in the possession of the
18 target person or in the conveyance in the course of the search
19 that the executing officer or person assisting believes on
20 reasonable grounds to be:

21 (i) prohibited goods that are unlawfully carried by the
22 target person; or

23 (ii) seizable items.

24 (2) A warrant that is in force in relation to a person (the *target person*)
25 authorises the executing officer or a person assisting:

26 (a) to use:

27 (i) a computer, or data storage device, found in the course
28 of a search authorised under the warrant; or

29 (ii) a telecommunications facility operated or provided by
30 the Commonwealth or a carrier; or

31 (iii) any other electronic equipment; or

32 (iv) a data storage device;

33 for the purpose of obtaining access to data (the *relevant data*)

34 that is held in the computer or device mentioned in

35 subparagraph (i) at any time when the warrant is in force, in

- 1 order to determine whether the relevant data is evidential
2 material of a kind specified in the warrant; and
3 (b) if necessary to achieve the purpose mentioned in
4 paragraph (a)—to add, copy, delete or alter other data in the
5 computer or device mentioned in subparagraph (a)(i); and
6 (c) if, having regard to other methods (if any) of obtaining access
7 to the relevant data which are likely to be as effective, it is
8 reasonable in all the circumstances to do so:
9 (i) to use any other computer or a communication in transit
10 to access the relevant data; and
11 (ii) if necessary to achieve that purpose—to add, copy,
12 delete or alter other data in the computer or the
13 communication in transit; and
14 (d) to copy any data to which access has been obtained, and that:
15 (i) appears to be relevant for the purposes of determining
16 whether the relevant data is evidential material of a kind
17 specified in the warrant; or
18 (ii) is evidential material of a kind specified in the warrant;
19 and
20 (e) to do any other thing reasonably incidental to any of the
21 above.

22 Note: As a result of the warrant, a person who, by means of a
23 telecommunications facility, obtains access to data stored in a
24 computer etc. will not commit an offence under Part 10.7 of the
25 *Criminal Code* or equivalent State or Territory laws (provided that the
26 person acts within the authority of the warrant).

- 27 (3) Subsection (2) does not authorise the addition, deletion or
28 alteration of data, or the doing of any thing, that is likely to:
29 (a) materially interfere with, interrupt or obstruct:
30 (i) a communication in transit; or
31 (ii) the lawful use by other persons of a computer;
32 unless the addition, deletion or alteration, or the doing of the
33 thing, is necessary to do one or more of the things specified
34 in the warrant; or
35 (b) cause any other material loss or damage to other persons
36 lawfully using a computer.

- 1 (4) It is immaterial whether a thing mentioned in subsection (2) is
2 done:
3 (a) in the presence of the target person; or
4 (b) at any other place.
- 5 (5) If the warrant states that it may be executed only during particular
6 hours, the warrant must not be executed outside those hours.
- 7 (6) If the warrant authorises an ordinary search or a frisk search of the
8 target person, a search of the target person different from that so
9 authorised must not be done under the warrant.

10 **5A Subsection 200(1)**

11 Omit “executing officer or a person assisting”, substitute “executing
12 officer of a warrant in relation to premises, or a person assisting”.

13 **5AA Subsection 200(2)**

14 Omit “thing found at the premises”, substitute “thing found at warrant
15 premises, or a thing found during a search under a warrant that is in
16 force in relation to a person”.

17 **5B Paragraph 200(2)(b)**

18 Repeal the paragraph, substitute:
19 (b) for a thing found at warrant premises—the occupier of the
20 premises consents in writing; or
21 (c) for a thing found during a search under a warrant that is in
22 force in relation to a person—the person consents in writing.

23 **5C Paragraph 200(3)(a)**

24 Omit “occupier”, substitute “person referred to in paragraph (2)(b) or
25 (c) (as the case requires)”.

26 **5D Paragraph 200(3)(b)**

27 Omit “the occupier”, substitute “that person”.

28 **6 Subsection 200(3A)**

29 Omit “72 hours.”, substitute:
30 whichever of the following is applicable:

- 1 (a) if the thing is a computer or data storage device—30 days;
2 (b) otherwise—72 hours.

3 **7 Subsection 200(3B)**

4 Omit “72 hours”, substitute “the time applicable under
5 subsection (3A)”.

6 **7A Subsection 200(3C)**

7 Omit “occupier of the premises, and the occupier”, substitute “person
8 referred to in paragraph (2)(b) or (c) (as the case requires), and that
9 person”.

10 **8 After subsection 200(3C)**

11 Insert:

12 (3D) If the thing is a computer or data storage device, a single extension
13 cannot exceed 14 days.

14 **8AA Subsection 200(4)**

15 Omit “executing officer or a person assisting”, substitute “executing
16 officer of a warrant in relation to premises, or a person assisting”.

17 **8A After section 201**

18 Insert:

19 **201AA Use of electronic equipment at other place**

- 20 (1) If electronic equipment is moved to another place under
21 subsection 200(2), the executing officer or a person assisting may
22 operate the equipment to access data (including data held at
23 another place).
- 24 (2) If the executing officer or person assisting suspects on reasonable
25 grounds that any data accessed by operating the electronic
26 equipment constitutes evidential material, the executing officer or
27 person assisting may copy any or all of the data accessed by
28 operating the electronic equipment to a disk, tape or other
29 associated device.

-
- 1 (3) If the Comptroller-General of Customs is satisfied that the data is
 2 not required (or is no longer required) for:
 3 (a) investigating an offence against a law of the Commonwealth,
 4 a State or a Territory; or
 5 (b) judicial proceedings or administrative review proceedings; or
 6 (c) investigating or resolving a complaint under the *Ombudsman*
 7 *Act 1976* or the *Privacy Act 1988*;
 8 the Comptroller-General of Customs must arrange for:
 9 (d) the removal of the data from any device subject to customs
 10 control; and
 11 (e) the destruction of any other reproduction of the data subject
 12 to customs control.
- 13 (4) If the executing officer or a person assisting, after operating the
 14 equipment, finds that evidential material is accessible by doing so,
 15 the executing officer or person assisting may:
 16 (a) seize the equipment and any disk, tape or other associated
 17 device; or
 18 (b) if the material can be put in documentary form—put the
 19 material in that form and seize the documents so produced.
- 20 (5) The executing officer or a person assisting may seize equipment
 21 under paragraph (4)(a) only if:
 22 (a) it is not practicable to copy the data as mentioned in
 23 subsection (2) or to put the material in documentary form as
 24 mentioned in paragraph (4)(b); or
 25 (b) possession of the equipment by the person referred to in
 26 paragraph 200(2)(b) or (c) (as the case requires) could
 27 constitute an offence.

28 **9 Paragraphs 201A(1)(a), (b) and (c)**

29 Repeal the paragraphs, substitute:

- 30 (a) access data held in, or accessible from, a computer or data
 31 storage device that:
 32 (i) is on warrant premises; or
 33 (ii) has been seized under this Subdivision; or
 34 (iii) is found in the course of an ordinary search of a person,
 35 or a frisk search of a person, authorised by a search
 36 warrant;
-

- 1 (b) copy data held in, or accessible from, a computer, or data
2 storage device, described in paragraph (a) to another data
3 storage device;
4 (c) convert into documentary form or another form intelligible to
5 an executing officer:
6 (i) data held in, or accessible from, a computer, or data
7 storage device, described in paragraph (a); or
8 (ii) data held in a data storage device to which the data was
9 copied as described in paragraph (b).

10 **10 Paragraph 201A(2)(a)**

11 After “the computer”, insert “or data storage device”.

12 **11 Subparagraph 201A(2)(b)(ii)**

13 After “the computer”, insert “or device”.

14 **12 Subparagraph 201A(2)(b)(iii)**

15 Omit “; and”, substitute “or device; or”.

16 **13 At the end of paragraph 201A(2)(b)**

17 Add:

- 18 (iv) a person engaged under a contract for services by the
19 owner or lessee of the computer or device; or
20 (v) a person who uses or has used the computer or device;
21 or
22 (vi) a person who is or was a system administrator for the
23 system including the computer or device; and

24 **14 Subparagraph 201A(2)(c)(i)**

25 After “the computer or”, insert “device or”.

26 **15 Subparagraph 201A(2)(c)(i)**

27 After “which the computer”, insert “or device”.

28 **16 Subparagraph 201A(2)(c)(i)**

29 After “forms”, insert “or formed”.

1 **17 Subparagraph 201A(2)(c)(ii)**

2 After “the computer”, insert “or device”.

3 **18 Subsection 201A(3)**

4 Repeal the subsection, substitute:

5 *Offences*

6 (3) A person commits an offence if:

- 7 (a) the person is subject to an order under this section; and
8 (b) the person is capable of complying with a requirement in the
9 order; and
10 (c) the person omits to do an act; and
11 (d) the omission contravenes the requirement.

12 Penalty: Imprisonment for 5 years or 300 penalty units, or both.

13 (4) A person commits an offence if:

- 14 (a) the person is subject to an order under this section; and
15 (b) the person is capable of complying with a requirement in the
16 order; and
17 (c) the person omits to do an act; and
18 (d) the omission contravenes the requirement; and
19 (e) the offence to which the relevant warrant relates is a serious
20 offence.

21 Penalty for contravention of this subsection: Imprisonment for 10
22 years or 600 penalty units, or both.

23 **18A Paragraph 201B(1)(a)**

24 After “201(1)”, insert “or 201AA(1)”.

25 **18B Paragraph 201B(1)(d)**

26 After “or (2)”, insert “or 201AA(2) or (4)”.

27 **18C Paragraph 202(1)(a)**

28 Omit “or 201”, substitute “, 201 or 201AA”.

1 **18D Paragraph 202A(2)(a)**

2 After “201(2)(b)”, insert “or 201AA(4)(a)”.

3 **18E At the end of Subdivision C of Division 1 of Part XII**

4 Add:

5 **202B Relationship of this Subdivision to parliamentary privileges**
6 **and immunities**

7 To avoid doubt, this Subdivision does not affect the law relating to
8 the powers, privileges and immunities of any of the following:

- 9 (a) each House of the Parliament;
10 (b) the members of each House of the Parliament;
11 (c) the committees of each House of the Parliament and joint
12 committees of both Houses of the Parliament.

13 **19 Subsection 203K(5)**

14 After “198(1),”, insert “199A(1),”.

15 **20 Subsection 203M(4)**

16 After “198,”, insert “199A,”.

17 **21 Application of amendments**

- 18 (1) The amendments of sections 199, 200 and 201A of the *Customs Act*
19 *1901* made by this Schedule apply in relation to a warrant issued after
20 the commencement of this item.
- 21 (2) Section 201AA of the *Customs Act 1901* (as amended by this Schedule)
22 applies in relation to a warrant issued after the commencement of this
23 item.

1 **Schedule 5—Australian Security Intelligence**
2 **Organisation**
3

4 *Australian Security Intelligence Organisation Act 1979*

5 **1 After subsection 16(1)**

6 Insert:

- 7 (1A) The Director-General may, by writing, delegate any or all of the
8 Director-General's functions or powers under section 21A to a
9 senior position-holder.

10 **2 At the end of Division 1 of Part III**

11 Add:

12 **21A Voluntary assistance provided to the Organisation**

13 *Assistance provided in accordance with a request by the*
14 *Director-General*

15 (1) If:

- 16 (a) the Director-General requests a person or body to engage in
17 conduct; and
18 (b) the Director-General is satisfied, on reasonable grounds, that
19 the conduct is likely to assist the Organisation in the
20 performance of its functions; and
21 (c) the person engages in the conduct in accordance with the
22 request; and
23 (d) the conduct does not involve the person or body committing
24 an offence against a law of the Commonwealth, a State or a
25 Territory; and
26 (e) the conduct does not result in significant loss of, or serious
27 damage to, property;
28 the person or body is not subject to any civil liability for, or in
29 relation to, the conduct.

30 (2) A request under paragraph (1)(a) may be made orally if:

- 1 (a) the Director-General is satisfied that the request should be
2 made as a matter of urgency; or
3 (b) the Director-General is satisfied that making the request in
4 writing would be prejudicial to security; or
5 (c) the Director-General is satisfied that making the request in
6 writing would be prejudicial to the operational security of the
7 Organisation.
- 8 (2A) If subsection (2) does not apply to a request under paragraph (1)(a),
9 the request must be made in writing.
- 10 (3) If a request under paragraph (1)(a) is made orally, the
11 Director-General must:
12 (a) make a written record of the request; and
13 (b) do so within 48 hours after the request was made.
- 14 (3A) If a request is made under paragraph (1)(a), the Director-General
15 must, within 7 days after the request is made, notify the
16 Inspector-General of Intelligence and Security that the request has
17 been made.
- 18 (4) The Director-General may enter into a contract, agreement or
19 arrangement with a person or body in relation to conduct engaged
20 in by the person or body in accordance with a request under
21 paragraph (1)(a).
- 22 *Unsolicited disclosure of information etc.*
- 23 (5) If:
24 (a) a person or body engages in conduct that consists of, or is
25 connected with:
26 (i) giving information to the Organisation; or
27 (ii) giving or producing a document to the Organisation; or
28 (iii) making one or more copies of a document and giving
29 those copies to the Organisation; and
30 (b) the person reasonably believes that the conduct is likely to
31 assist the Organisation in the performance of its functions;
32 and

- 1 (c) the conduct does not involve the person or body committing
2 an offence against a law of the Commonwealth, a State or a
3 Territory; and
4 (d) the conduct does not result in significant loss of, or serious
5 damage to, property; and
6 (e) subsection (1) does not apply to the conduct;
7 the person or body is not subject to any civil liability for, or in
8 relation to, the conduct.

9 *Copies of, or extracts from, documents*

- 10 (6) The Organisation may make and retain copies of, or take and retain
11 extracts from, a document given or produced to the Organisation:
12 (a) in accordance with a request under paragraph (1)(a); or
13 (b) under paragraph (5)(a).

14 *Subsections (1) and (5) have effect despite other laws*

- 15 (7) Subsections (1) and (5) have effect despite anything in a law of the
16 Commonwealth, a State or a Territory (whether passed or made
17 before or after the commencement of this section) unless the law
18 expressly provides otherwise.

19 *Certificate*

- 20 (8) The Director-General may give a certificate in writing certifying
21 one or more facts relevant to the question of whether the
22 Director-General was satisfied, on reasonable grounds, that
23 particular conduct was likely to assist the Organisation in the
24 performance of its functions.
25 (9) In any proceedings that involve determining whether subsection (1)
26 or (5) applies to particular conduct, a certificate given under
27 subsection (8) is prima facie evidence of the facts certified.

28 *Compensation for acquisition of property*

- 29 (10) If the operation of this section would result in an acquisition of
30 property (within the meaning of paragraph 51(xxxi) of the
31 Constitution) from a person otherwise than on just terms (within

1 the meaning of that paragraph), the Commonwealth is liable to pay
2 a reasonable amount of compensation to the person.

3 (11) If the Commonwealth and the person do not agree on the amount
4 of the compensation, the person may institute proceedings in the
5 Federal Court of Australia for the recovery from the
6 Commonwealth of such reasonable amount of compensation as the
7 court determines.

8 **2A After subsection 34(1)**

9 Insert:

10 (1A) If an order was made under subsection 34AAA(2) in relation to the
11 warrant, the report must also include details of the extent to which
12 compliance with the order has assisted the Organisation in carrying
13 out its functions.

14 **3 At the end of Division 2 of Part III**

15 Add:

16 **Subdivision J—Assistance relating to access to data**

17 **34AAA Person with knowledge of a computer or a computer system**
18 **to assist access to data**

19 (1) The Director-General may request the Attorney-General to make
20 an order requiring a specified person to provide any information or
21 assistance that is reasonable and necessary to allow the
22 Organisation to do one or more of the following:

23 (a) access data held in, or accessible from, a computer or data
24 storage device that:

25 (i) is the subject of a warrant under section 25A, 26 or
26 27A; or

27 (ii) is the subject of an authorisation under section 27E or
28 27F; or

29 (iii) is on premises in relation to which a warrant under
30 section 25, 26 or 27A is in force; or

31 (iv) is on premises in relation to which an authorisation
32 under section 27D or 27F is in force; or

- 1 (v) is found in the course of an ordinary search of a person,
- 2 or a frisk search of a person, authorised by a warrant
- 3 under section 25 or 27A; or
- 4 (vi) is found in the course of an ordinary search of a person,
- 5 or a frisk search of a person, authorised under
- 6 section 27D; or
- 7 (vii) has been removed from premises under a warrant under
- 8 section 25, 26 or 27A; or
- 9 (viii) has been removed from premises under section 27D; or
- 10 (ix) has been seized under section 34ZB;
- 11 (b) copy data held in, or accessible from, a computer, or data
- 12 storage device, described in paragraph (a) to another data
- 13 storage device;
- 14 (c) convert into documentary form or another form intelligible to
- 15 an ASIO employee or ASIO affiliate:
 - 16 (i) data held in, or accessible from, a computer, or data
 - 17 storage device, described in paragraph (a); or
 - 18 (ii) data held in a data storage device to which the data was
 - 19 copied as described in paragraph (b); or
 - 20 (iii) data held in a computer or data storage device removed
 - 21 from premises under a warrant under section 25, 26 or
 - 22 27A; or
 - 23 (iv) data held in a computer or data storage device removed
 - 24 from premises under section 27D.
- 25 (2) The Attorney-General may make the order if:
 - 26 (a) in a case where the computer or data storage device:
 - 27 (i) is the subject of a warrant under section 27A; or
 - 28 (ii) is on premises in relation to which a warrant under
 - 29 section 27A is in force; or
 - 30 (iii) is found in the course of an ordinary search of a person,
 - 31 or a frisk search of a person, authorised by a warrant
 - 32 under section 27A; or
 - 33 (iv) has been removed from premises under a warrant under
 - 34 section 27A;
 the Attorney-General is satisfied, on reasonable grounds,
 that:

- 1 (v) access by the Organisation to data held in, or accessible
2 from, the computer or data storage device will be for the
3 purpose of obtaining foreign intelligence relating to a
4 matter specified in the relevant notice under
5 subsection 27A(1); and
- 6 (vi) on the basis of advice received from the Defence
7 Minister or the Foreign Affairs Minister, the collection
8 of foreign intelligence relating to that matter is in the
9 interests of Australia's national security, Australia's
10 foreign relations or Australia's national economic
11 well-being; and
- 12 (b) in a case where paragraph (a) does not apply—the
13 Attorney-General is satisfied that there are reasonable
14 grounds for suspecting that access by the Organisation to data
15 held in, or accessible from, the computer or data storage
16 device will substantially assist the collection of intelligence
17 in accordance with this Act in respect of a matter that is
18 important in relation to security; and
- 19 (c) the Attorney-General is satisfied, on reasonable grounds, that
20 the specified person is:
- 21 (i) reasonably suspected of being involved in activities that
22 are prejudicial to security; or
- 23 (ii) the owner or lessee of the computer or device; or
- 24 (iii) an employee of the owner or lessee of the computer or
25 device; or
- 26 (iv) a person engaged under a contract for services by the
27 owner or lessee of the computer or device; or
- 28 (v) a person who uses or has used the computer or device;
29 or
- 30 (vi) a person who is or was a system administrator for the
31 system including the computer or device; and
- 32 (d) the Attorney-General is satisfied, on reasonable grounds, that
33 the specified person has relevant knowledge of:
- 34 (i) the computer or device or a computer network of which
35 the computer or device forms or formed a part; or
- 36 (ii) measures applied to protect data held in, or accessible
37 from, the computer or device.

-
- 1 (3) If the computer or data storage device is not on premises in relation
2 to which a warrant is in force, the order must:
- 3 (a) specify the period within which the person must provide the
4 information or assistance; and
- 5 (b) specify the place at which the person must provide the
6 information or assistance; and
- 7 (c) specify the conditions (if any) determined by the
8 Attorney-General as the conditions to which the requirement
9 on the person to provide the information or assistance is
10 subject.
- 11 (3A) A request under subsection (1) may be made:
- 12 (a) orally; or
13 (b) in writing.
- 14 (3B) If a request under subsection (1) is made orally, the
15 Director-General must:
- 16 (a) make a written record of the request; and
17 (b) do so within 48 hours after the request was made.
- 18 (3C) A request under subsection (1) (the *current request*) must be
19 accompanied by a statement setting out the particulars and
20 outcomes of all previous requests (if any) under that subsection for
21 the making of an order relating to the person specified in the
22 current request.
- 23 (3D) If the Director-General is satisfied that the grounds on which an
24 order under this section was made have ceased to exist, the
25 Director-General must, as soon as practicable, inform the
26 Attorney-General of that fact.
- 27 (3E) If:
- 28 (a) an order is in force under this section; and
29 (b) the Attorney-General is satisfied that the grounds on which
30 the order was made have ceased to exist;
31 the Attorney-General must revoke the order.
- 32 (4) A person commits an offence if:
33 (a) the person is subject to an order under this section; and

- 1 (b) the person is capable of complying with a requirement in the
2 order; and
3 (c) the person omits to do an act; and
4 (d) the omission contravenes the requirement.

5 Penalty for contravention of this subsection: Imprisonment for 5
6 years or 300 penalty units, or both.

7 **4 Section 34ZH**

8 Before “The Director-General”, insert “(1)”.

9 **5 At the end of section 34ZH**

10 Add:

- 11 (2) If an order was made under subsection 34AAA(2) in relation to
12 accessing data that was held in, or accessible from, a computer or
13 storage device that was seized under section 34ZB, the report must
14 also include details of the extent to which compliance with the
15 order has assisted the Organisation in carrying out its functions.

16 **6 Before subsection 94(2C)**

17 Insert:

- 18 (2BC) A report under subsection (1) must also include a statement of:
19 (a) the total number of requests made under paragraph 21A(1)(a)
20 during the period; and
21 (b) the total number of orders made under subsection 34AAA(2)
22 during the period.
23

(204/18)
