

2016-2017-2018

The Parliament of the
Commonwealth of Australia

HOUSE OF REPRESENTATIVES

Presented and read a first time

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

No. , 2018

(Attorney-General)

**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>Criminal Code Act 1995</i>		4
<i>Telecommunications Act 1997</i>		5
Part 2—Amendments contingent on the commencement of the Federal Circuit and Family Court of Australia Act 2018		68
<i>Telecommunications Act 1997</i>		68
Schedule 2—Computer access warrants etc.		69
Part 1—Amendments		69
<i>Australian Security Intelligence Organisation Act 1979</i>		69
<i>Mutual Assistance in Criminal Matters Act 1987</i>		74
<i>Surveillance Devices Act 2004</i>		76
<i>Telecommunications Act 1997</i>		129
<i>Telecommunications (Interception and Access) Act 1979</i>		129
Part 2—Application provisions		139
Part 3—Amendments contingent on the commencement of the Crimes Legislation Amendment (International Crime Cooperation and Other Measures) Act 2018		140
<i>International Criminal Court Act 2002</i>		140
<i>International War Crimes Tribunals Act 1995</i>		141
<i>Surveillance Devices Act 2004</i>		142
Schedule 3—Search warrants issued under the Crimes Act 1914		146
<i>Crimes Act 1914</i>		146

Schedule 4—Search warrants issued under the Customs Act 1901	155
<i>Customs Act 1901</i>	155
Schedule 5—Australian Security Intelligence Organisation	167
<i>Australian Security Intelligence Organisation Act 1979</i>	167

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	A single day to be fixed by Proclamation. However, if the provisions do not commence within the period of 9 months beginning on the day this Act receives the Royal Assent, they commence on the day after the end of that period.	
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.	

Commencement information

Column 1	Column 2	Column 3
Provisions	Commencement	Date/Details
6. Schedules 3, 4 and 5	The day after this Act receives the Royal Assent.	

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

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

7 **3 Schedules**

8 Legislation that is specified in a Schedule to this Act is amended or
9 repealed as set out in the applicable items in the Schedule
10 concerned, and any other item in a Schedule to this Act has effect
11 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 *Criminal Code Act 1995*

8 **2 After subsection 474.6(7) of the *Criminal Code***

9 Insert:

10 (7A) A person is not criminally responsible for an offence against
11 subsection (5) if the conduct of the person:

12 (a) is in accordance with a technical assistance request; or

13 (b) is in compliance with a technical assistance notice; or

14 (c) is in compliance with a technical capability notice.

15 **3 After subparagraph 476.2(4)(b)(iii) of the *Criminal Code***

16 Insert:

17 or (iv) in accordance with a technical assistance request; or

18 (v) in compliance with a technical assistance notice; or

19 (vi) in compliance with a technical capability notice;

20 **4 Dictionary in the *Criminal Code***

21 Insert:

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

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

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

1 ***Telecommunications Act 1997***

2 **5 Section 7**

3 Insert:

4 *ASIO* means the Australian Security Intelligence Organisation.

5 **6 Section 7 (paragraph (a) of the definition of *civil penalty***
6 ***provision*)**

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

8 **7 After Part 14**

9 Insert:

10 **Part 15—Industry assistance**

11 **Division 1—Introduction**

12 **317A Simplified outline of this Part**

- 13
- 14
- 15
- 16
- 17
- 18
- 19
- 20
- 21
- 22
- 23
- 24
- 25
- 26
- 27
- 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.
 - 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) enforcing the criminal law and laws imposing pecuniary penalties; or
 - (b) assisting the enforcement of the criminal laws in force in a foreign country; 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

- (c) the interests of Australia’s national security, the interests of Australia’s foreign relations or the interests of Australia’s national economic well-being.

- 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) enforcing the criminal law and laws imposing pecuniary penalties; or
 - (b) assisting the enforcement of the criminal laws in force in a foreign country; or
 - (c) the interests of Australia’s national security, the interests of Australia’s foreign relations or the interests of Australia’s national economic well-being.

- 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 help to ASIO or the agency in relation to:
 - (a) enforcing the criminal law and laws imposing pecuniary penalties; or
 - (b) assisting the enforcement of the criminal laws in force in a foreign country; 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 and laws imposing pecuniary penalties; or
 - (b) assisting the enforcement of the criminal laws in force in a foreign country; or
 - (c) safeguarding national security.

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- A technical capability notice may require the provider to do acts or things by way of giving help to ASIO or an interception agency in relation to:
 - (a) enforcing the criminal law and laws imposing pecuniary penalties; or
 - (b) assisting the enforcement of the criminal laws in force in a foreign country; or
 - (c) safeguarding national security.

9 **317B Definitions**

10 In this Part:

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

- 12 (a) access that is subject to a pre-condition (for example, the use
- 13 of a password); and
- 14 (b) access by way of push technology; and
- 15 (c) access by way of a standing request.

16 ***ASIO affiliate*** has the same meaning as in the *Australian Security*

17 *Intelligence Organisation Act 1979*.

18 ***ASIO employee*** has the same meaning as in the *Australian Security*

19 *Intelligence Organisation Act 1979*.

20 ***chief officer*** of an interception agency has the meaning given by

21 section 317ZM.

22 ***contracted service provider***, in relation to a designated

23 communications provider, means a person who performs services

24 for or on behalf of the provider, but does not include a person who

25 performs such services in the capacity of an employee of the

26 provider.

27 ***Corruption and Crime Commission (WA)*** means the Corruption

28 and Crime Commission established by the *Corruption, Crime and*

29 *Misconduct Act 2003 (WA)*.

30 ***designated communications provider*** has the meaning given by

31 section 317C.

- 1 ***electronic service*** has the meaning given by section 317D.
- 2 ***eligible activities*** of a designated communications provider has the
3 meaning given by section 317C.
- 4 ***entrusted ASD person*** means a person who:
- 5 (a) is a staff member of the Australian Signals Directorate; or
6 (b) has entered into a contract, agreement or arrangement with
7 the Australian Signals Directorate; or
8 (c) is an employee or agent of a person who has entered into a
9 contract, agreement or arrangement with the Australian
10 Signals Directorate.
- 11 ***entrusted ASIO person*** means an entrusted person (within the
12 meaning of the *Australian Security Intelligence Organisation Act*
13 *1979*).
- 14 ***entrusted ASIS person*** means a person who:
- 15 (a) is a staff member or agent of the Australian Secret
16 Intelligence Service; or
17 (b) has entered into a contract, agreement or arrangement with
18 the Australian Secret Intelligence Service; or
19 (c) is an employee or agent of a person who has entered into a
20 contract, agreement or arrangement with the Australian
21 Secret Intelligence Service.
- 22 ***giving help:***
- 23 (a) when used in relation to ASIO—includes giving help to an
24 ASIO employee or an ASIO affiliate; or
25 (b) when used in relation to the Australian Secret Intelligence
26 Service—includes giving help to a staff member of the
27 Australian Secret Intelligence Service; or
28 (c) when used in relation to the Australian Signals Directorate—
29 includes giving help to a staff member of the Australian
30 Signals Directorate; or
31 (d) when used in relation to an interception agency—includes
32 giving help to an officer of the agency.
- 33 ***IGIS official*** has the same meaning as in the *Australian Security*
34 *Intelligence Organisation Act 1979*.

1 ***Independent Broad-based Anti-corruption Commission of***
2 ***Victoria*** means the Independent Broad-based Anti-corruption
3 Commission established by the *Independent Broad-based*
4 *Anti-corruption Commission Act 2011* (Vic).

5 ***Independent Commissioner Against Corruption (SA)*** means the
6 person who is the Commissioner (within the meaning of the
7 *Independent Commissioner Against Corruption Act 2012* (SA)).

8 ***interception agency*** means:

- 9 (a) the Australian Federal Police; or
10 (b) the Australian Commission for Law Enforcement Integrity;
11 or
12 (c) the Australian Crime Commission; or
13 (d) the Police Force of a State or the Northern Territory; or
14 (e) the Independent Commission Against Corruption of New
15 South Wales; or
16 (f) the New South Wales Crime Commission; or
17 (g) the Law Enforcement Conduct Commission of New South
18 Wales; or
19 (h) the Independent Broad-based Anti-corruption Commission of
20 Victoria; or
21 (i) the Crime and Corruption Commission of Queensland; or
22 (j) the Independent Commissioner Against Corruption (SA); or
23 (k) the Corruption and Crime Commission (WA).

24 ***Law Enforcement Conduct Commission of New South Wales***
25 means the Law Enforcement Conduct Commission constituted by
26 the *Law Enforcement Conduct Commission Act 2016* (NSW).

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

28 ***material*** means material:

- 29 (a) whether in the form of text; or
30 (b) whether in the form of data; or
31 (c) whether in the form of speech, music or other sounds; or
32 (d) whether in the form of visual images (moving or otherwise);
33 or
34 (e) whether in any other form; or
-

1 (f) whether in any combination of forms.

2 **member of the staff of the Independent Commissioner Against**
3 **Corruption (SA)** means a person who is engaged under
4 subsection 12(1) of the *Independent Commissioner Against*
5 *Corruption Act 2012 (SA)*.

6 **officer** of an interception agency has the meaning given by
7 section 317ZM.

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

11 **supply**:

12 (a) when used in relation to:

13 (i) a facility; or

14 (ii) customer equipment; or

15 (iii) a component;

16 includes supply (including re-supply) by way of sale,
17 exchange, lease, hire or hire-purchase; and

18 (b) when used in relation to software—includes provide, grant or
19 confer rights, privileges or benefits.

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

22 **technical assistance notice information** means:

23 (a) information about any of the following:

24 (i) the giving of a technical assistance notice;

25 (ii) the existence or non-existence of a technical assistance
26 notice;

27 (iii) the variation of a technical assistance notice;

28 (iv) the revocation of a technical assistance notice;

29 (v) the requirements imposed by a technical assistance
30 notice;

31 (vi) any act or thing done in compliance with a technical
32 assistance notice; or

33 (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 (v) the revocation of a technical capability notice;
 - 24 (vi) the requirements imposed by a technical capability
25 notice;
 - 26 (vii) any act or thing done in compliance with a technical
27 capability notice; or
- 28 (b) any other information about a technical capability notice.

29 **317C Designated communications provider etc.**

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

- 31 (a) ***designated communications provider***; and
32 (b) the ***eligible activities*** of a designated communications
33 provider.

34

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 ...
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 or more end-users 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
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

Designated communications provider and eligible activities		
Item	A person is a designated communications provider if and the eligible activities of the person are ...
		(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
13	the person: (a) connects customer equipment to a telecommunications network in Australia; and	any such connection by the person of customer equipment to a telecommunications network in Australia

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 ...
	(b) does so otherwise than in the capacity of end-user of the equipment	
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
2 advice to designated communications providers).

3 Note 2: See also section 317ZT (alternative constitutional basis).

4 **317D Electronic service**

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

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

- 1 (b) a service that delivers material to persons having equipment
2 appropriate for receiving that material, where the delivery of
3 the service is by means of a carriage service;
4 but does not include:
5 (c) a broadcasting service; or
6 (d) a datacasting service (within the meaning of the
7 *Broadcasting Services Act 1992*).
- 8 (2) For the purposes of subsection (1), *service* includes a website.
- 9 (3) For the purposes of this Part, a person does not provide an
10 electronic service merely because the person supplies a carriage
11 service that enables material to be accessed or delivered.
- 12 (4) For the purposes of this Part, a person does not provide an
13 electronic service merely because the person provides a billing
14 service, or a fee collection service, in relation to an electronic
15 service.
- 16 (5) A reference in this section to the *use* of a thing is a reference to the
17 use of the thing either:
18 (a) in isolation; or
19 (b) in conjunction with one or more other things.

20 **317E Listed acts or things**

- 21 (1) For the purposes of the application of this Part to a designated
22 communications provider, *listed act or thing* means:
23 (a) removing one or more forms of electronic protection that are
24 or were applied by, or on behalf of, the provider; or
25 (b) providing technical information; or
26 (c) installing, maintaining, testing or using software or
27 equipment; or
28 (d) ensuring that information obtained in connection with the
29 execution of a warrant or authorisation is given in a particular
30 format; or
31 (e) facilitating or assisting access to whichever of the following
32 are the subject of eligible activities of the provider:
33 (i) a facility;
34 (ii) customer equipment;
-

Schedule 1 Industry assistance
Part 1 Amendments

- 1 (iii) a data processing device;
2 (iv) a listed carriage service;
3 (v) a service that facilitates, or is ancillary or incidental to,
4 the supply of a listed carriage service;
5 (vi) an electronic service;
6 (vii) a service that facilitates, or is ancillary or incidental to,
7 the provision of an electronic service;
8 (viii) software used, for use, or likely to be used, in
9 connection with a listed carriage service;
10 (ix) software used, for use, or likely to be used, in
11 connection with an electronic service;
12 (x) software that is capable of being installed on a
13 computer, or other equipment, that is, or is likely to be,
14 connected to a telecommunications network; or
15 (f) assisting with the testing, modification, development or
16 maintenance of a technology or capability; or
17 (g) notifying particular kinds of changes to, or developments
18 affecting, eligible activities of the designated
19 communications provider, if the changes are relevant to the
20 execution of a warrant or authorisation; or
21 (h) modifying, or facilitating the modification of, any of the
22 characteristics of a service provided by the designated
23 communications provider; or
24 (i) substituting, or facilitating the substitution of, a service
25 provided by the designated communications provider for:
26 (i) another service provided by the provider; or
27 (ii) a service provided by another designated
28 communications provider; or
29 (j) an act or thing done to conceal the fact that any thing has
30 been done covertly in the performance of a function, or the
31 exercise of a power, conferred by a law of the
32 Commonwealth, a State or a Territory, so far as the function
33 or power relates to:
34 (i) enforcing the criminal law and laws imposing pecuniary
35 penalties; or
36 (ii) assisting the enforcement of the criminal laws in force
37 in a foreign country; or

- 1 (iii) the interests of Australia's national security, the
2 interests of Australia's foreign relations or the interests
3 of Australia's national economic well-being.

4 (2) Paragraph (1)(j) does not apply to:

- 5 (a) making a false or misleading statement; or
6 (b) engaging in dishonest conduct.

7 **317F Extension to external Territories**

8 This Part extends to every external Territory.

9 **Division 2—Voluntary technical assistance**

10 **317G Voluntary technical assistance provided to ASIO, the**
11 **Australian Secret Intelligence Service, the Australian**
12 **Signals Directorate or an interception agency**

13 (1) If:

14 (a) any of the following persons:

- 15 (i) the Director-General of Security;
16 (ii) the Director-General of the Australian Secret
17 Intelligence Service;
18 (iii) the Director-General of the Australian Signals
19 Directorate;

20 (iv) the chief officer of an interception agency;
21 requests a designated communications provider to do one or
22 more specified acts or things that:

23 (v) are in connection with any or all of the eligible activities
24 of the provider; and

25 (vi) are covered by subsection (2); and

26 (b) the provider does an act or thing:

- 27 (i) in accordance with the request; or
28 (ii) in good faith purportedly in accordance with the
29 request;

30 then:

31 (c) the provider is not subject to any civil liability for, or in
32 relation to, the act or thing mentioned in paragraph (b); and

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

- 1 (v) the performance of a function, or the exercise of a
2 power, conferred by or under a law of the
3 Commonwealth, a State or a Territory, so far as the
4 function or power relates to a relevant objective; or
5 (vi) a matter that facilitates, or is ancillary or incidental to, a
6 matter covered by subparagraph (v).

7 (3) A request under paragraph (1)(a) is to be known as a *technical*
8 *assistance request*.

9 (4) Subparagraph (1)(b)(ii) does not apply to an act or thing done by a
10 designated communications provider unless the act or thing is in
11 connection with any or all of the eligible activities of the provider.

12 *Relevant objective*

- 13 (5) For the purposes of this section, *relevant objective* means:
14 (a) enforcing the criminal law and laws imposing pecuniary
15 penalties; or
16 (b) assisting the enforcement of the criminal laws in force in a
17 foreign country; or
18 (c) the interests of Australia's national security, the interests of
19 Australia's foreign relations or the interests of Australia's
20 national economic well-being.

21 *Listed acts or things*

- 22 (6) The acts or things that may be specified in a technical assistance
23 request given to a designated communications provider include
24 (but are not limited to) listed acts or things, so long as those acts or
25 things:
26 (a) are in connection with any or all of the eligible activities of
27 the provider; and
28 (b) are covered by subsection (2).

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

30 **317H Form of technical assistance request**

- 31 (1) A technical assistance request may be given:
32 (a) orally; or
-

- 1 (b) in writing.
- 2 (2) A technical assistance request must not be given orally unless:
- 3 (a) an imminent risk of serious harm to a person or substantial
- 4 damage to property exists; and
- 5 (b) the technical assistance request is necessary for the purpose
- 6 of dealing with that risk; and
- 7 (c) it is not practicable in the circumstances to give the technical
- 8 assistance request in writing.
- 9 (3) If a technical assistance request is given orally by:
- 10 (a) the Director-General of Security; or
- 11 (b) the Director-General of the Australian Secret Intelligence
- 12 Service; or
- 13 (c) the Director-General of the Australian Signals Directorate; or
- 14 (d) the chief officer of an interception agency;
- 15 the Director-General of Security, the Director-General of the
- 16 Australian Secret Intelligence Service, the Director-General of the
- 17 Australian Signals Directorate or the chief officer, as the case
- 18 requires, must:
- 19 (e) make a written record of the request; and
- 20 (f) do so within 48 hours after the request was given.
- 21 (4) If, under subsection (3):
- 22 (a) the Director-General of Security; or
- 23 (b) the Director-General of the Australian Secret Intelligence
- 24 Service; or
- 25 (c) the Director-General of the Australian Signals Directorate; or
- 26 (d) the chief officer of an interception agency;
- 27 makes a written record of a technical assistance request, the
- 28 Director-General of Security, the Director-General of the
- 29 Australian Secret Intelligence Service, the Director-General of the
- 30 Australian Signals Directorate or the chief officer, as the case
- 31 requires, must:
- 32 (e) give a copy of the record to the designated communications
- 33 provider concerned; and
- 34 (f) do so as soon as practicable after the record was made.

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 **317HA Duration of technical assistance request**

- 22 (1) A technical assistance request:
23 (a) comes in force:
24 (i) when it is given; or
25 (ii) if a later time is specified in the request—at that later
26 time; and
27 (b) unless sooner revoked, remains in force:
28 (i) if an expiry date is specified in the request—until the
29 start of the expiry date; or
30 (ii) otherwise—at end of the 90-day period beginning when
31 the request was given.
- 32 (2) If a technical assistance request expires, this Part does not prevent
33 the giving of a fresh technical assistance request in the same terms
34 as the expired technical assistance request.

1 **317J Specified period etc.**

- 2 (1) A technical assistance request may include a request that a
3 specified act or thing be done within a specified period.
- 4 (2) A technical assistance request may include a request that a
5 specified act or thing be done:
6 (a) in a specified manner; or
7 (b) in a way that meets one or more specified conditions.
- 8 (3) Subsections (1) and (2) of this section do not limit
9 subsections 317G(1) and (2).

10 **317JA Variation of technical assistance requests**

- 11 (1) If a technical assistance request has been given to a designated
12 communications provider by the Director-General of Security, the
13 Director-General of Security may vary the request.
- 14 (2) If a technical assistance request has been given to a designated
15 communications provider by the Director-General of the Australian
16 Secret Intelligence Service, the Director-General of the Australian
17 Secret Intelligence Service may vary the request.
- 18 (3) If a technical assistance request has been given to a designated
19 communications provider by the Director-General of the Australian
20 Signals Directorate, the Director-General of the Australian Signals
21 Directorate may vary the request.
- 22 (4) If a technical assistance request has been given to a designated
23 communications provider by the chief officer of an interception
24 agency, the chief officer may vary the request.

25 *Form of variation*

- 26 (5) A variation may be made:
27 (a) orally; or
28 (b) in writing.
- 29 (6) A variation must not be made orally unless:
30 (a) an imminent risk of serious harm to a person or substantial
31 damage to property exists; and

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

- 1 (10) The acts or things that may be specified in a varied technical
2 assistance request include (but are not limited to) listed acts or
3 things, so long as those acts or things:
4 (a) are in connection with any or all of the eligible activities of
5 the designated communications provider concerned; and
6 (b) are covered by subsection 317G(2).

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

8 **317JB Revocation of technical assistance requests**

- 9 (1) If a technical assistance request has been given to a person by the
10 Director-General of Security, the Director-General of Security
11 may, by written notice given to the person, revoke the request.
- 12 (2) If a technical assistance request has been given to a person by the
13 Director-General of the Australian Secret Intelligence Service, the
14 Director-General of the Australian Secret Intelligence Service may,
15 by written notice given to the person, revoke the request.
- 16 (3) If a technical assistance request has been given to a person by the
17 Director-General of the Australian Signals Directorate, the
18 Director-General of the Australian Signals Directorate may, by
19 written notice given to the person, revoke the request.
- 20 (4) If a technical assistance request has been given to a person by the
21 chief officer of an interception agency, the chief officer may, by
22 written notice given to the person, revoke the request.

23 **317K Contract etc.**

24 Any of the following persons:

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

30 may enter into a contract, agreement or arrangement with a
31 designated communications provider in relation to acts or things
32 done by the provider in accordance with a technical assistance
33 request.

1 **Division 3—Technical assistance notices**

2 **317L Technical assistance notices**

3 (1) The Director-General of Security or the chief officer of an
4 interception agency may give a designated communications
5 provider a notice, to be known as a technical assistance notice, that
6 requires the provider to do one or more specified acts or things
7 that:

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

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

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

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

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

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

18 in relation to:

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

22 (i) enforcing the criminal law and laws imposing pecuniary
23 penalties; or

24 (ii) assisting the enforcement of the criminal laws in force
25 in a foreign country; or

26 (iii) safeguarding national security; or

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

29 *Listed acts or things*

30 (3) The acts or things that may be specified in a technical assistance
31 notice given to a designated communications provider include (but
32 are not limited to) listed acts or things, so long as those acts or
33 things:

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

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

5 **317M Form of technical assistance notice**

- 6 (1) A technical assistance notice may be given:
7 (a) orally; or
8 (b) in writing.
- 9 (2) A technical assistance notice must not be given orally unless:
10 (a) an imminent risk of serious harm to a person or substantial
11 damage to property exists; and
12 (b) the technical assistance notice is necessary for the purpose of
13 dealing with that risk; and
14 (c) it is not practicable in the circumstances to give the technical
15 assistance notice in writing.
- 16 (3) If a technical assistance notice is given orally by the
17 Director-General of Security or the chief officer of an interception
18 agency, the Director-General of Security or the chief officer, as the
19 case requires, must:
20 (a) make a written record of the notice; and
21 (b) do so within 48 hours after the notice was given.
- 22 (4) If, under subsection (3), the Director-General of Security or the
23 chief officer of an interception agency makes a written record of a
24 technical assistance notice, the Director-General of Security or the
25 chief officer, as the case requires, must:
26 (a) give a copy of the record to the designated communications
27 provider concerned; and
28 (b) do so as soon as practicable after the record was made.

29 **317MAA Provision of advice to designated communications**
30 **providers**

- 31 (1) If the Director-General of Security gives a technical assistance
32 notice to a designated communications provider, the
33 Director-General of Security must give the provider advice relating
-

1 to the provider's obligations under whichever of sections 317ZA
2 and 317ZB is applicable, so far as those obligations relate to the
3 notice.

4 (2) If the chief officer of an interception agency gives a technical
5 assistance notice to a designated communications provider, the
6 chief officer must give the provider advice relating to the
7 provider's obligations under whichever of sections 317ZA and
8 317ZB is applicable, so far as those obligations relate to the notice.

9 **317MA Duration of technical assistance notice**

- 10 (1) A technical assistance notice:
11 (a) comes in force:
12 (i) when it is given; or
13 (ii) if a later time is specified in the notice—at that later
14 time; and
15 (b) unless sooner revoked, remains in force:
16 (i) if an expiry date is specified in the notice—until the
17 start of the expiry date; or
18 (ii) otherwise—at end of the 90-day period beginning when
19 the notice was given.
- 20 (2) If a technical assistance notice expires, this Part does not prevent
21 the giving of a fresh technical assistance notice in the same terms
22 as the expired technical assistance notice.

23 **317N Compliance period etc.**

- 24 (1) A technical assistance notice may require a specified act or thing to
25 be done within a specified period.
- 26 (2) A technical assistance notice may require a specified act or thing to
27 be done:
28 (a) in a specified manner; or
29 (b) in a way that meets one or more specified conditions.
- 30 (3) Subsections (1) and (2) of this section do not limit
31 subsections 317L(1) and (2).

1 **317P Decision-making criteria**

2 The Director-General of Security or the chief officer of an
3 interception agency must not give a technical assistance notice to a
4 designated communications provider unless the Director-General
5 of Security or the chief officer, as the case requires, is satisfied
6 that:

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

12 Note: See also section 317RA.

13 **317Q Variation of technical assistance notices**

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

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

20 *Form of variation*

21 (3) A variation may be made:

- 22 (a) orally; or
23 (b) in writing.

24 (4) A variation must not be made orally unless:

- 25 (a) an imminent risk of serious harm to a person or substantial
26 damage to property exists; and
27 (b) the variation is necessary for the purpose of dealing with that
28 risk; and
29 (c) it is not practicable in the circumstances to make the
30 variation in writing.

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

20 *Acts or things specified in a varied technical assistance notice*

- 21 (8) The acts or things specified in a varied technical assistance notice
22 must be:
23 (a) in connection with any or all of the eligible activities of the
24 designated communications provider concerned; and
25 (b) covered by subsection 317L(2).
- 26 (9) The acts or things that may be specified in a varied technical
27 assistance notice include (but are not limited to) listed acts or
28 things, so long as those acts or things:
29 (a) are in connection with any or all of the eligible activities of
30 the designated communications provider concerned; and
31 (b) are covered by subsection 317L(2).

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

1 *Decision-making criteria*

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

11 Note: See also section 317RA.

12 **317R Revocation of technical assistance notices**

- 13 (1) If a technical assistance notice has been given to a person by the
14 Director-General of Security, the Director-General of Security
15 may, by written notice given to the person, revoke the notice.
- 16 (2) If a technical assistance notice has been given to a person by the
17 Director-General of Security, and the Director-General of Security
18 is satisfied that:
19 (a) the requirements imposed by the notice are not reasonable
20 and proportionate; or
21 (b) compliance with the notice is not:
22 (i) practicable; and
23 (ii) technically feasible;
24 the Director-General of Security must, by written notice given to
25 the person, revoke the notice.
- 26 (3) If a technical assistance notice has been given to a person by the
27 chief officer of an interception agency, the chief officer may, by
28 written notice given to the person, revoke the notice.
- 29 (4) If a technical assistance notice has been given to a person by the
30 chief officer of an interception agency, and the chief officer is
31 satisfied that:
32 (a) the requirements imposed by the notice are not reasonable
33 and proportionate; or
34 (b) compliance with the notice is not:
-

- 1 (i) practicable; and
2 (ii) technically feasible;
3 the chief officer must, by written notice given to the person, revoke
4 the notice.

5 **317RA Whether requirements imposed by a technical assistance**
6 **notice are reasonable and proportionate**

7 In considering whether the requirements imposed by a technical
8 assistance notice or a varied technical assistance notice are
9 reasonable and proportionate, the Director-General of Security or
10 the chief officer of an interception agency, as the case requires,
11 must have regard to the following matters:

- 12 (a) the interests of national security;
13 (b) the interests of law enforcement;
14 (c) the legitimate interests of the designated communications
15 provider to whom the notice relates;
16 (d) the objectives of the notice;
17 (e) the availability of other means to achieve the objectives of
18 the notice;
19 (f) the legitimate expectations of the Australian community
20 relating to privacy and cybersecurity;
21 (g) such other matters (if any) as the Director-General of
22 Security or the chief officer, as the case requires, considers
23 relevant.

24 **Division 4—Technical capability notices**

25 **317S Attorney-General may determine procedures and**
26 **arrangements relating to requests for technical capability**
27 **notices**

- 28 (1) The Attorney-General may, by writing, determine procedures and
29 arrangements to be followed in relation to the making of requests
30 for technical capability notices.
31 (2) A procedure or arrangement determined under subsection (1) may
32 require that the agreement of a person or body must be obtained
33 before a request is made for a technical capability notice.

1 (3) A failure to comply with a determination under subsection (1) does
2 not affect the validity of a technical capability notice.

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

5 **317T Technical capability notices**

6 (1) The Attorney-General may, in accordance with a request made by
7 the Director-General of Security or the chief officer of an
8 interception agency, give a designated communications provider a
9 written notice, to be known as a technical capability notice, that
10 requires the provider to do one or more specified acts or things
11 that:

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

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

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

17 (2) The specified acts or things must:

18 (a) be directed towards ensuring that the designated
19 communications provider is capable of giving listed help to
20 ASIO, or an interception agency, in relation to:

21 (i) the performance of a function, or the exercise of a
22 power, conferred by or under a law of the
23 Commonwealth, a State or a Territory, so far as the
24 function or power relates to a relevant objective; or

25 (ii) a matter that facilitates, or is ancillary or incidental to, a
26 matter covered by subparagraph (i); or

27 (b) be by way of giving help to ASIO, or an interception agency,
28 in relation to:

29 (i) the performance of a function, or the exercise of a
30 power, conferred by or under a law of the
31 Commonwealth, a State or a Territory, so far as the
32 function or power relates to a relevant objective; or

33 (ii) a matter that facilitates, or is ancillary or incidental to, a
34 matter covered by subparagraph (i).

1 *Relevant objective*

- 2 (3) For the purposes of this section, **relevant objective** means:
- 3 (a) enforcing the criminal law and laws imposing pecuniary
- 4 penalties; or
- 5 (b) assisting the enforcement of the criminal laws in force in a
- 6 foreign country; or
- 7 (c) safeguarding national security.

8 *Listed help*

- 9 (4) For the purposes of the application of this section to a designated
- 10 communications provider, if one or more acts or things done by the
- 11 provider:
- 12 (a) are by way of giving help to ASIO or an interception agency;
- 13 and
- 14 (b) are in connection with any or all of the eligible activities of
- 15 the provider; and
- 16 (c) consist of either or both of the following:
- 17 (i) one or more listed acts or things (other than an act or
- 18 thing covered by paragraph 317E(1)(a));
- 19 (ii) one or more acts or things of a kind determined under
- 20 subsection (5);

21 that help is **listed help**.

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

- 23 (5) The Minister may, by legislative instrument, determine one or
- 24 more kinds of acts or things for the purposes of
- 25 subparagraph (4)(c)(ii).
- 26 (6) In making a determination under subsection (5), the Minister must
- 27 have regard to the following matters:
- 28 (a) the interests of law enforcement;
- 29 (b) the interests of national security;
- 30 (c) the objects of this Act;
- 31 (d) the likely impact of the determination on designated
- 32 communications providers;
- 33 (e) such other matters (if any) as the Minister considers relevant.

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

Listed acts or things

- (7) The acts or things that may be specified in a technical capability notice given to a designated communications provider in accordance with paragraph (2)(b) include (but are not limited to) listed acts or things, so long as those acts or things:
- (a) are in connection with any or all of the eligible activities of the provider; and
 - (b) are covered by subsection (2), so far as that subsection relates to paragraph (2)(b).

Limits

- (8) If:
- (a) a designated communications provider supplies a particular kind of telecommunications service; and
 - (b) the service involves, or will involve, the use of a telecommunications system;
- a technical capability notice has no effect to the extent (if any) to which it requires the provider to ensure that the kind of service, or the system:
- (c) has the capability to enable a communication passing over the system to be intercepted in accordance with an interception warrant; or
 - (d) has the capability to transmit lawfully intercepted information to the delivery points applicable in respect of that kind of service; or
 - (e) has a delivery capability.
- Note 1: Part 5-3 of the *Telecommunications (Interception and Access) Act 1979* deals with interception capability.
- Note 2: Part 5-5 of the *Telecommunications (Interception and Access) Act 1979* deals with delivery capability.
- (9) For the purposes of subsection (8), ensuring that a kind of service or a system has a particular capability includes ensuring that the capability is developed, installed and maintained.
- (10) A technical capability notice has no effect to the extent (if any) to which it requires a designated communications provider to keep, or cause to be kept:

- 1 (a) information of a kind specified in or under section 187AA of
2 the *Telecommunications (Interception and Access) Act 1979*;
3 or
4 (b) documents containing information of that kind;
5 relating to any communication carried by means of a service to
6 which Part 5-1A of the *Telecommunications (Interception and*
7 *Access) Act 1979* applies.

8 Note: Part 5-1A of the *Telecommunications (Interception and Access) Act*
9 *1979* deals with data retention.

- 10 (11) An expression used in subsection (8), (9) or (10) of this section and
11 in Chapter 5 of the *Telecommunications (Interception and Access)*
12 *Act 1979* has the same meaning in those subsections as it has in
13 that Chapter.

14 *Applicable costs negotiator*

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

17 Note: See section 317ZK.

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

22 **317TAA Provision of advice to designated communications** 23 **providers**

24 If the Attorney-General gives a technical capability notice to a
25 designated communications provider, the Attorney-General must
26 give the provider advice relating to the provider's obligations
27 under whichever of sections 317ZA and 317ZB is applicable, so
28 far as those obligations relate to the notice.

29 **317TA Duration of technical capability notice**

- 30 (1) A technical capability notice:
31 (a) comes in force:
32 (i) when it is given; or
-

- 1 (ii) if a later time is specified in the notice—at that later
2 time; and
3 (b) unless sooner revoked, remains in force:
4 (i) if an expiry date is specified in the notice—until the
5 start of the expiry date; or
6 (ii) otherwise—at end of the 180-day period beginning
7 when the notice was given.
- 8 (2) If a technical capability notice expires, this Part does not prevent
9 the giving of a fresh technical capability notice in the same terms
10 as the expired technical capability notice.

11 **317U Compliance period etc.**

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

20 **317V Decision-making criteria**

- 21 The Attorney-General must not give a technical capability notice to
22 a designated communications provider unless:
23 (a) the Attorney-General is satisfied that the requirements
24 imposed by the notice are reasonable and proportionate; and
25 (b) the Attorney-General is satisfied that compliance with the
26 notice is:
27 (i) practicable; and
28 (ii) technically feasible.
- 29 Note: See also section 317ZAA.

1 **317W Consultation about a proposal to give a technical capability**
2 **notice**

- 3 (1) The Attorney-General must not give a technical capability notice to
4 a designated communications provider unless the Attorney-General
5 has first:
6 (a) given the provider a written notice (the *consultation notice*):
7 (i) setting out a proposal to give the technical capability
8 notice; and
9 (ii) inviting the provider to make a submission to the
10 Attorney-General on the proposed technical capability
11 notice; and
12 (b) considered any submission that was received within the time
13 limit specified in the consultation notice; and
14 (c) considered any copy of a report given to the
15 Attorney-General under subsection (7) within the time limit
16 specified in the consultation notice.
- 17 (2) A time limit specified in a consultation notice must run for at least
18 28 days.
- 19 (3) The rule in subsection (2) does not apply to a technical capability
20 notice given to a designated communications provider if:
21 (a) the Attorney-General is satisfied that the technical capability
22 notice should be given as a matter of urgency; or
23 (b) compliance with subsection (2) is impracticable; or
24 (c) the provider waives compliance with subsection (2).
- 25 (4) For the purposes of paragraph (3)(c), a designated communications
26 provider may waive compliance:
27 (a) orally; or
28 (b) in writing.
- 29 (5) If compliance is waived orally by a designated communications
30 provider, the provider must:
31 (a) make a written record of the waiver; and
32 (b) do so within 48 hours after the waiver was made.
- 33 (6) If, under subsection (5), a designated communications provider
34 makes a written record of the waiver, the provider must:

- 1 (a) give a copy of the record to the Attorney-General; and
2 (b) do so as soon as practicable after the record was made.

3 *Assessment and report—section 317ZG*

- 4 (7) If the Attorney-General gives a consultation notice to a designated
5 communications provider, the Attorney-General and the provider
6 may jointly appoint one or more persons to:
7 (a) carry out an assessment of whether the proposed technical
8 capability notice would contravene section 317ZG; and
9 (b) prepare a report of the assessment; and
10 (c) give copies of the report to:
11 (i) the Attorney-General; and
12 (ii) the provider;
13 within the time limit specified in the consultation notice.
- 14 (8) A person must not be appointed under subsection (7) unless the
15 person has knowledge that would enable the person to assess
16 whether the proposed technical capability notice would contravene
17 section 317ZG.
- 18 (9) An appointment of one or more persons under subsection (7) is
19 taken to be made on the basis that the designated communications
20 provider has agreed to be responsible for paying the remuneration
21 of those persons.
- 22 (10) The Attorney-General may, on behalf of the Commonwealth,
23 reimburse the whole or part of the amount of any remuneration
24 paid by a designated communications provider to a person or
25 persons appointed under subsection (7).
- 26 (11) For the purposes of this Part:
27 (a) information about the carrying out of an assessment under
28 subsection (7); or
29 (b) information contained in a report prepared under
30 subsection (7);
31 is taken to be information about consultation relating to the giving
32 of a technical capability notice.

1 **317X Variation of technical capability notices**

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

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

- 6 (2) The acts or things specified in a varied technical capability notice
7 must be:
8 (a) in connection with any or all of the eligible activities of the
9 designated communications provider concerned; and
10 (b) covered by subsection 317T(2).
- 11 (3) The acts or things that may be specified in a varied technical
12 capability notice in accordance with paragraph 317T(2)(b) include
13 (but are not limited to) listed acts or things, so long as those acts or
14 things:
15 (a) are in connection with any or all of the eligible activities of
16 the designated communications provider concerned; and
17 (b) are covered by subsection 317T(2), so far as that subsection
18 relates to paragraph 317T(2)(b).

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

20 *Decision-making criteria*

- 21 (4) The Attorney-General must not vary a technical capability notice
22 unless the Attorney-General is satisfied that:
23 (a) the requirements imposed by the varied notice are reasonable
24 and proportionate; and
25 (b) compliance with the varied notice is:
26 (i) practicable; and
27 (ii) technically feasible.

28 Note: See also section 317ZAA.

1 **317Y Consultation about a proposal to vary a technical capability**
2 **notice**

- 3 (1) If a technical capability notice has been given to a designated
4 communications provider, the Attorney-General must not vary the
5 notice unless the Attorney-General has first:
6 (a) given the provider a written notice (the *consultation notice*):
7 (i) setting out a proposal to vary the technical capability
8 notice; and
9 (ii) inviting the provider to make a submission to the
10 Attorney-General on the proposed variation; and
11 (b) considered any submission that was received within the time
12 limit specified in the consultation notice.
- 13 (2) A time limit specified in a consultation notice must run for at least
14 28 days.
- 15 (3) If a technical capability notice has been given to a designated
16 communications provider, the rule in subsection (2) does not apply
17 to a variation of the notice if:
18 (a) the Attorney-General is satisfied that the technical capability
19 notice should be varied as a matter of urgency; or
20 (b) compliance with subsection (2) is impracticable; or
21 (c) the provider waives compliance with subsection (2).
- 22 (4) For the purposes of paragraph (3)(c), a designated communications
23 provider may waive compliance:
24 (a) orally; or
25 (b) in writing.
- 26 (5) If compliance is waived orally by a designated communications
27 provider, the provider must:
28 (a) make a written record of the waiver; and
29 (b) do so within 48 hours after the waiver was made.
- 30 (6) If, under subsection (5), a designated communications provider
31 makes a written record of the waiver, the provider must:
32 (a) give a copy of the record to the Attorney-General; and
33 (b) do so as soon as practicable after the record was made.

1 **317Z Revocation of technical capability notices**

- 2 (1) If a technical capability notice has been given to a person, the
3 Attorney-General may, by written notice given to the person,
4 revoke the notice.
- 5 (2) If a technical capability notice has been given to a person, and the
6 Attorney-General is satisfied that:
- 7 (a) the requirements imposed by the notice are not reasonable
8 and proportionate; or
 - 9 (b) compliance with the notice is not:
 - 10 (i) practicable; and
 - 11 (ii) technically feasible;
- 12 the Attorney-General must, by written notice given to the person,
13 revoke the 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 (f) the legitimate expectations of the Australian community
28 relating to privacy and cybersecurity;
- 29 (g) such other matters (if any) as the Attorney-General considers
30 relevant.

1 **Division 5—Compliance and enforcement**

2 **317ZA Compliance with notices—carriers and carriage service**
3 **providers**

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

19 Note: Part 31 provides for pecuniary penalties for breaches of civil penalty
20 provisions.

21 **317ZB Compliance with notices—designated communications**
22 **provider (other than a carrier or carriage service**
23 **provider)**

- 24 (1) A designated communications provider (other than a carrier or
25 carriage service provider) must comply with a requirement under:
26 (a) a technical assistance notice; or
27 (b) a technical capability notice;
28 to the extent that the provider is capable of doing so.
- 29 Civil penalty:
30 (a) if the provider is a body corporate—47,619 penalty units; or
31 (b) if the provider is not a body corporate—238 penalty units.

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

20 **317ZC Civil penalty provision**

21 *Enforceable civil penalty provision*

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

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

28 *Authorised applicant*

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

1 *Relevant courts*

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

6 *Extension to external Territories etc.*

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

11 **317ZD Enforceable undertakings**

12 *Enforceable provision*

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

15 *Authorised person*

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

19 *Relevant courts*

20 (3) The Federal Court and the Federal Circuit Court of Australia are
21 relevant courts in relation to section 317ZB of this Act for the
22 purposes of Part 6 of the *Regulatory Powers (Standard Provisions)*
23 *Act 2014*.

24 *Extension to external Territories etc.*

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

1 **317ZE Injunctions**

2 *Enforceable provision*

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

5 *Authorised person*

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

9 *Relevant courts*

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

14 *Extension to external Territories etc.*

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

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

20 **317ZF Unauthorised disclosure of information**

- 21 (1) A person commits an offence if:
22 (a) the person discloses information; and
23 (b) the person is or was:
24 (i) a designated communications provider; or
25 (ii) an employee of a designated communications provider;
26 or
27 (iii) a contracted service provider of a designated
28 communications provider; or

Schedule 1 Industry assistance
Part 1 Amendments

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

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

1 *Exceptions*

2 (2) Subsection (1) does not apply if the disclosure was authorised
3 under subsection (3), (5), (6), (7), (8), (9), (10), (11) or (13).

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

6 *Authorised disclosures—general*

- 7 (3) A person covered by paragraph (1)(b) may disclose technical
8 assistance notice information, technical capability notice
9 information or technical assistance request information:
10 (a) in connection with the administration or execution of this
11 Part; or
12 (b) for the purposes of any legal proceedings arising out of or
13 otherwise related to this Part or of any report of any such
14 proceedings; or
15 (c) in accordance with any requirement imposed by a law of the
16 Commonwealth, a State or a Territory; or
17 (d) in connection with the performance of functions, or the
18 exercise of powers, by:
19 (i) ASIO; or
20 (ii) the Australian Secret Intelligence Service; or
21 (iii) the Australian Signals Directorate; or
22 (iv) an interception agency; or
23 (e) for the purpose of obtaining legal advice in relation to this
24 Part; or
25 (f) to an IGIS official for the purpose of exercising powers, or
26 performing functions or duties, as an IGIS official.
27 (4) For the purposes of subsection (3), *this Part* includes:
28 (a) any other provision of this Act, so far as that other provision
29 relates to this Part; and
30 (b) the *Regulatory Powers (Standard Provisions) Act 2014*, so
31 far as that Act relates to this Part.

32 *Authorised disclosures—IGIS official*

- 33 (5) An IGIS official may disclose:
34 (a) technical assistance notice information; or
-

- 1 (b) technical capability notice information; or
2 (c) technical assistance request information;
3 in connection with the IGIS official exercising powers, or
4 performing functions or duties, as an IGIS official.

5 *Authorised disclosures—information sharing*

- 6 (6) The Director-General of Security or the Communications Access
7 Co-ordinator may disclose information that is:
8 (a) technical assistance notice information; or
9 (b) technical capability notice information; or
10 (c) technical assistance request information;
11 to the chief officer of an interception agency for purposes relating
12 to the performance of functions, or the exercise of powers, by the
13 interception agency.
- 14 (7) The chief officer of an interception agency may disclose
15 information that is:
16 (a) technical assistance notice information; or
17 (b) technical capability notice information; or
18 (c) technical assistance request information;
19 to the chief officer of another interception agency for purposes
20 relating to the performance of functions, or the exercise of powers,
21 by the other interception agency.
- 22 (8) The Director-General of Security, the Director-General of the
23 Australian Signals Directorate or the chief officer of an
24 interception agency 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 Director-General of the Australian Secret Intelligence
29 Service for purposes relating to the performance of functions, or
30 the exercise of powers, by the Australian Secret Intelligence
31 Service.
- 32 (9) The Director-General of Security, the Director-General of the
33 Australian Secret Intelligence Service or the chief officer of an
34 interception agency may disclose information that is:
-

- 1 (a) technical assistance notice information; or
2 (b) technical capability notice information; or
3 (c) technical assistance request information;
4 to the Director-General of the Australian Signals Directorate for
5 purposes relating to the performance of functions, or the exercise
6 of powers, by the Australian Signals Directorate.
- 7 (10) The Communications Access Co-ordinator, the Director-General of
8 the Australian Secret Intelligence Service, the Director-General of
9 the Australian Signals Directorate or the chief officer of an
10 interception agency may disclose information that is:
11 (a) technical assistance notice information; or
12 (b) technical capability notice information; or
13 (c) technical assistance request information;
14 to the Director-General of Security for purposes relating to the
15 performance of functions, or the exercise of powers, by ASIO.
- 16 (11) The Director-General of Security or the chief officer of an
17 interception agency may disclose information that is:
18 (a) technical assistance notice information; or
19 (b) technical capability notice information; or
20 (c) technical assistance request information;
21 to the Communications Access Co-ordinator for purposes relating
22 to the performance of functions, or the exercise of powers, by the
23 Communications Access Co-ordinator.
- 24 (12) Before disclosing information under subsection (6), (7), (8), (9) or
25 (10), the Director-General of Security, the Director-General of the
26 Australian Secret Intelligence Service, the Director-General of the
27 Australian Signals Directorate or the chief officer of an
28 interception agency, as the case requires, must notify the
29 Communications Access Co-ordinator of the proposed disclosure.
- 30 *Authorised disclosures—statistics*
- 31 (13) A person who is:
32 (a) a designated communications provider; or
33 (b) an employee of a designated communications provider; or

- 1 (c) a contracted service provider of a designated communications
2 provider; or
3 (d) an employee of a contracted service provider of a designated
4 communications provider;
5 may, in the person's capacity as such a provider or employee,
6 disclose:
7 (e) the total number of technical assistance notices given to the
8 provider during a period of at least 6 months; or
9 (f) the total number of technical capability notices given to the
10 provider during a period of at least 6 months; or
11 (g) the total number of technical assistance requests given to the
12 provider during a period of at least 6 months.
- 13 Note: This subsection authorises the disclosure of aggregate statistical
14 information. That information cannot be broken down:
15 (a) by agency; or
16 (b) in any other way.

17 **317ZFA Powers of a court**

- 18 (1) In a proceeding under, or arising out of:
19 (a) this Part; or
20 (b) any other provision of this Act, so far as that other provision
21 relates to this Part; or
22 (c) the *Regulatory Powers (Standard Provisions) Act 2014*, so
23 far as that Act relates to this Part;
24 a court may make such orders as the court considers appropriate in
25 relation to the disclosure, protection, storage, handling or
26 destruction, in the proceeding, of:
27 (d) technical assistance notice information; or
28 (e) technical capability notice information; or
29 (f) technical assistance request information;
30 if the court is satisfied that it is in the public interest to make such
31 orders.
- 32 (2) The powers conferred on a court by subsection (1) are in addition
33 to any other powers of the court.

1 **Division 7—Limitations**

2 **317ZG Designated communications provider must not be required**
3 **to implement or build a systemic weakness or systemic**
4 **vulnerability etc.**

- 5 (1) A technical assistance notice or technical capability notice must
6 not have the effect of:
- 7 (a) requiring a designated communications provider to
8 implement or build a systemic weakness, or a systemic
9 vulnerability, into a form of electronic protection; or
 - 10 (b) preventing a designated communications provider from
11 rectifying a systemic weakness, or a systemic vulnerability,
12 in a form of electronic protection.
- 13 (2) The reference in paragraph (1)(a) to implement or build a systemic
14 weakness, or a systemic vulnerability, into a form of electronic
15 protection includes a reference to implement or build a new
16 decryption capability in relation to a form of electronic protection.
- 17 (3) The reference in paragraph (1)(a) to implement or build a systemic
18 weakness, or a systemic vulnerability, into a form of electronic
19 protection includes a reference to one or more actions that would
20 render systemic methods of authentication or encryption less
21 effective.
- 22 (4) Subsections (2) and (3) are enacted for the avoidance of doubt.
- 23 (5) A technical assistance notice or technical capability notice has no
24 effect to the extent (if any) to which it would have an effect
25 covered by paragraph (1)(a) or (b).

26 **317ZH General limits on technical assistance notices and technical**
27 **capability notices**

- 28 (1) A technical assistance notice or technical capability notice has no
29 effect to the extent (if any) to which it would require a designated
30 communications provider to do an act or thing for which a warrant
31 or authorisation under any of the following laws is required:
- 32 (a) the *Telecommunications (Interception and Access) Act 1979*;
 - 33 (b) the *Surveillance Devices Act 2004*;

- 1 (c) the *Crimes Act 1914*;
- 2 (d) the *Australian Security Intelligence Organisation Act 1979*;
- 3 (e) the *Intelligence Services Act 2001*;
- 4 (f) a law of the Commonwealth (other than this Part) that is not
- 5 covered by paragraph (a), (b), (c), (d) or (e);
- 6 (g) a law of a State or Territory.
- 7 (2) For the purposes of subsection (1):
- 8 (a) assume that each law mentioned in that subsection applied
- 9 both within and outside Australia; and
- 10 (b) assume that each reference in Part 13 to a carriage service
- 11 provider included a reference to a designated
- 12 communications provider.
- 13 (3) A technical assistance notice or technical capability notice has no
- 14 effect to the extent (if any) to which it would require a designated
- 15 communications provider to:
- 16 (a) use a surveillance device (within the meaning of the
- 17 *Surveillance Devices Act 2004*); or
- 18 (b) access data held in a computer (within the meaning of the
- 19 *Surveillance Devices Act 2004*);
- 20 if a law of a State or Territory requires a warrant or authorisation
- 21 for that use or access.
- 22 (4) To avoid doubt, subsection (1) or (3) does not prevent a technical
- 23 assistance notice or technical capability notice from requiring a
- 24 designated communications provider to do an act or thing by way
- 25 of giving help to:
- 26 (a) ASIO; or
- 27 (b) an interception agency;
- 28 in relation to:
- 29 (c) in the case of a technical assistance notice—a matter covered
- 30 by paragraph 317L(2)(c) or (d); or
- 31 (d) in the case of a technical capability notice—a matter covered
- 32 by subparagraph 317T(2)(b)(i) or (ii);
- 33 if the doing of the act or thing would:
- 34 (e) assist in, or facilitate, giving effect to a warrant or
- 35 authorisation under a law of the Commonwealth, a State or a
- 36 Territory; or
-

- 1 (f) give effect to a warrant or authorisation under a law of the
2 Commonwealth.
- 3 (5) To avoid doubt, subsection (1) or (3) does not prevent a technical
4 capability notice from requiring a designated communications
5 provider to do an act or thing directed towards ensuring that the
6 provider is capable of giving listed help (within the meaning of
7 section 317T) to:
- 8 (a) ASIO; or
9 (b) an interception agency;
10 in relation to a matter covered by subparagraph 317T(2)(a)(i) or
11 (ii), if the doing of the act or thing would:
- 12 (c) assist in, or facilitate, giving effect to a warrant or
13 authorisation under a law of the Commonwealth, a State or a
14 Territory; or
15 (d) give effect to a warrant or authorisation under a law of the
16 Commonwealth.

17 **Division 8—General provisions**

18 **317ZJ Immunity**

- 19 (1) A designated communications provider is not subject to any civil
20 liability for, or in relation to, an act or thing done by the provider:
- 21 (a) in compliance; or
22 (b) in good faith in purported compliance;
23 with:
- 24 (c) a technical assistance notice; or
25 (d) a technical capability notice.
- 26 (2) Paragraph (1)(b) does not apply to an act or thing done by a
27 designated communications provider unless the act or thing is in
28 connection with any or all of the eligible activities of the provider.
- 29 (3) An officer, employee or agent of a designated communications
30 provider is not subject to any civil liability for, or in relation to, an
31 act or thing done by the officer, employee or agent in connection
32 with an act or thing done by the provider:
- 33 (a) in compliance; or

- 1 (b) in good faith in purported compliance;
2 with:
3 (c) a technical assistance notice; or
4 (d) a technical capability notice.
- 5 (4) Paragraph (3)(b) does not apply to an act or thing done by a
6 designated communications provider unless the act or thing is in
7 connection with any or all of the eligible activities of the provider.

8 **317ZK Terms and conditions on which help is to be given etc.**

9 *Scope*

- 10 (1) This section applies if a designated communications provider is
11 subject to a requirement under:
12 (a) a technical assistance notice; or
13 (b) a technical capability notice;
14 unless:
15 (c) in the case of a requirement under a technical assistance
16 notice given by the Director-General of Security—the
17 Director-General of Security is satisfied that it would be
18 contrary to the public interest for this section to apply to the
19 requirement; or
20 (d) in the case of a requirement under a technical assistance
21 notice given by the chief officer of an interception agency—
22 the chief officer is satisfied that it would be contrary to the
23 public interest for this section to apply to the requirement; or
24 (e) in the case of a requirement under a technical capability
25 notice—the Attorney-General is satisfied that it would be
26 contrary to the public interest for this section to apply to the
27 requirement.
- 28 (2) In deciding whether it would be contrary to the public interest for
29 this section to apply to a requirement, the Director-General of
30 Security, the chief officer or the Attorney-General, as the case may
31 be, must have regard to the following matters:
32 (a) the interests of law enforcement;
33 (b) the interests of national security;
34 (c) the objects of this Act;

- 1 (d) the extent to which compliance with the requirement will
2 impose a regulatory burden on the provider;
3 (e) the reasons for the giving of the technical assistance notice or
4 technical capability notice, as the case requires;
5 (f) such other matters (if any) as the Director-General of
6 Security, the chief officer or the Attorney-General, as the
7 case may be, considers relevant.

8 *Basis of compliance*

- 9 (3) The designated communications provider must comply with the
10 requirement on the basis that the provider neither:
11 (a) profits from complying with the requirement; nor
12 (b) bears the reasonable costs of complying with the
13 requirement;
14 unless the provider and the applicable costs negotiator otherwise
15 agree.

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

17 *Terms and conditions*

- 18 (4) The designated communications provider must comply with the
19 requirement on such terms and conditions as are:
20 (a) agreed between the following parties:
21 (i) the provider;
22 (ii) the applicable costs negotiator; or
23 (b) failing agreement, determined by an arbitrator appointed by
24 the parties.

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

- 26 (5) If:
27 (a) the parties fail to agree on the appointment of an arbitrator;
28 and
29 (b) one of the parties is a carrier or carriage service provider;
30 the ACMA is to appoint the arbitrator.

- 31 (6) If:
32 (a) the parties fail to agree on the appointment of an arbitrator;
33 and

1 (b) none of the parties is a carrier or carriage service provider;
2 the Attorney-General is to appoint the arbitrator.

3 *Arbitration*

4 (7) An arbitrator appointed under subsection (5) or (6) must be:

5 (a) a person specified under subsection (8); or

6 (b) a person who belongs to a class of persons specified under
7 subsection (11).

8 (8) The Minister may, by writing, specify one or more persons for the
9 purposes of paragraph (7)(a).

10 (9) An instrument made under subsection (8) is not a legislative
11 instrument.

12 (10) Subsection 33(3AB) of the *Acts Interpretation Act 1901* does not
13 apply to the power conferred by subsection (8).

14 (11) The Minister may, by legislative instrument, specify a class of
15 persons for the purposes of paragraph (7)(b).

16 (12) Before making an instrument under subsection (8) or (11), the
17 Minister must consult the Attorney-General.

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

21 (14) The Minister may, by legislative instrument, make provision for
22 and in relation to the conduct of an arbitration under this section.

23 *Acquisition of property*

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

28 *Applicable costs negotiator*

29 (16) For the purposes of this section, the *applicable costs negotiator* is:

- 1 (a) in the case of a requirement under a technical assistance
2 notice given by the Director-General of Security—the
3 Director-General of Security; or
4 (b) 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; or
7 (c) in the case of a requirement under a technical capability
8 notice—the person specified in the notice, in accordance with
9 subsection 317T(12), as the applicable costs negotiator for
10 the notice.

11 **317ZL Service of notices etc.**

12 *Scope*

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

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

- 25 (2) If:
26 (a) the summons, process or notice, as the case may be, is
27 required to be served on, or given to, a designated
28 communications provider; and
29 (b) the designated communications provider has nominated an
30 address for service in a document given by the provider to:
31 (i) the Attorney-General; or
32 (ii) the Communications Access Co-ordinator; or
33 (iii) the Director-General of Security; or
34 (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

Schedule 1 Industry assistance
Part 1 Amendments

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
2	Australian Commission for Law Enforcement Integrity	the Integrity Commissioner (within the meaning of the <i>Law Enforcement Integrity Commissioner Act 2006</i>)	(a) the Integrity Commissioner (within the meaning of the <i>Law Enforcement Integrity Commissioner Act 2006</i>); or (b) a staff member of ACLEI (within the meaning of the <i>Law Enforcement Integrity</i>

Chief officer and officers of interception agencies			
Item	Column 1	Column 2	Column 3
	Interception agency	Chief officer	Officer
			<i>Commissioner Act 2006)</i>
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 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
5	Independent Commission Against Corruption of New South Wales	the Chief Commissioner (within the meaning of the <i>Independent Commission Against Corruption Act 1988</i> (NSW))	an officer of the Commission (within the meaning of the <i>Independent Commission Against Corruption Act 1988</i> (NSW)) (other than a person engaged under section 104B of that Act)
6	New South Wales Crime Commission	the Commissioner (within the meaning of the <i>Crime Commission Act 2012</i> (NSW))	an officer of the Commission (within the meaning of the <i>Crime Commission Act 2012</i> (NSW)) other than a person engaged under subsection 74(2)

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 that Act
7	Law Enforcement Conduct Commission of New South Wales	the Chief Commissioner (within the meaning of the <i>Law Enforcement Conduct Commission Act 2016</i> (NSW))	(a) the Chief Commissioner (within the meaning of the <i>Law Enforcement Conduct Commission Act 2016</i> (NSW)); or (b) the Commissioner for Integrity (within the meaning of the <i>Law Enforcement Conduct Commission Act 2016</i> (NSW)); or (c) a member of the staff of the Commission (within the meaning of the <i>Law Enforcement Conduct Commission Act 2016</i> (NSW))
8	Independent Broad-based Anti-corruption Commission of Victoria	the Commissioner (within the meaning of the <i>Independent Broad-based Anti-corruption Commission Act 2011</i> (Vic.))	a sworn IBAC Officer (within the meaning of the <i>Independent Broad-based Anti-corruption Commission Act 2011</i> (Vic.))
9	Crime and Corruption Commission of Queensland	the chairperson (within the meaning of the <i>Crime and Corruption Act 2001</i> (Qld))	a commission officer (as defined by paragraph (a) of the definition of commission officer in the Dictionary to the

Chief officer and officers of interception agencies			
Item	Column 1	Column 2	Column 3
	Interception agency	Chief officer	Officer
			<i>Crime and Corruption Act 2001 (Qld)</i> other than a person engaged under section 256 of that Act
10	Independent Commissioner Against Corruption (SA)	the Commissioner (within the meaning of the <i>Independent Commissioner Against Corruption Act 2012</i> (SA))	(a) the Commissioner (within the meaning of the <i>Independent Commissioner Against Corruption Act 2012</i> (SA)); or (b) the Deputy Commissioner; or (c) a member of the staff of the Independent Commissioner Against Corruption (SA)
11	Corruption and Crime Commission (WA)	the Commissioner (within the meaning of the <i>Corruption, Crime and Misconduct Act 2003</i> (WA))	an officer of the Commission (within the meaning of the <i>Corruption, Crime and Misconduct Act 2003</i> (WA)) other than a person engaged under section 182 of that Act

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.

1 **317ZP Delegation by Director-General of the Australian Secret**
2 **Intelligence Service**

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

7 (a) is a staff member of the Australian Secret Intelligence
8 Service; and

9 (b) holds, or is acting in, a position in the Australian Secret
10 Intelligence Service that is equivalent to, or higher than, a
11 position occupied by an SES employee.

12 (2) A delegate must comply with any written directions of the
13 Director-General of the Australian Secret Intelligence Service.

14 **317ZQ Delegation by Director-General of the Australian Signals**
15 **Directorate**

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

20 (a) who is a staff member of the Australian Signals Directorate;
21 and

22 (b) who:

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

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

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

30 **317ZR Delegation by the chief officer of an interception agency**

31 (1) The chief officer of an interception agency mentioned in an item of
32 column 1 of the following table may, by writing, delegate any or

1 all of the functions or powers of the chief officer under Division 2,
2 3 or 6 to a person mentioned in column 2 of the item.

3

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>)
2	Australian Commission for Law Enforcement Integrity	(a) an Assistant Integrity Commissioner (within the meaning of the <i>Law Enforcement Integrity Commissioner Act 2006</i>); or (b) a staff member of ACLEI (within the meaning of the <i>Law Enforcement Integrity Commissioner Act 2006</i>) who is an SES employee or acting SES employee
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 Northern Territory	(a) an Assistant Commissioner of the Police Force or a person holding equivalent rank; or (b) a Superintendent of the Police Force or a person holding equivalent rank
5	Independent Commission Against Corruption of New South Wales	(a) a Commissioner (within the meaning of the <i>Independent Commission Against Corruption Act 1988 (NSW)</i>); or (b) an Assistant Commissioner (within the meaning of the <i>Independent Commission Against Corruption Act 1988 (NSW)</i>); or (c) an officer of the Commission (within the meaning of the <i>Independent Commission Against Corruption Act 1988 (NSW)</i>) (other than a person engaged under section 104B of that Act) who is at executive level
6	New South Wales Crime Commission	an officer of the Commission (within the meaning of the <i>Crime Commission Act 2012 (NSW)</i>) (other than a person engaged under subsection 74(2) of that Act) who is at executive level
7	Law	(a) the Commissioner for Integrity (within the meaning

Schedule 1 Industry assistance
Part 1 Amendments

Potential delegates

Item	Column 1	Column 2
	Interception agency	Potential delegates
	Enforcement Conduct Commission of New South Wales	of the <i>Law Enforcement Conduct Commission Act 2016</i> (NSW)); or (b) a member of the staff of the Commission (within the meaning of the <i>Law Enforcement Conduct Commission Act 2016</i> (NSW)) who is at executive level
8	Independent Broad-based Anti-corruption Commission of Victoria	(a) a Deputy Commissioner of the Commission; or (b) the Chief Executive Officer of the Commission; or (c) a sworn IBAC Officer (within the meaning of the <i>Independent Broad-based Anti-corruption Commission Act 2011</i> (Vic.)) who is at executive level
9	Crime and Corruption Commission of Queensland	a senior executive officer (within the meaning of the <i>Crime and Corruption Act 2001</i> (Qld))
10	Independent Commissioner Against Corruption (SA)	(a) the Deputy Commissioner; or (b) a member of the staff of the Independent Commissioner Against Corruption who is at executive level

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

1 executive (within the meaning of the *Public Administration Act*
2 *2004* (Vic.)).

3 (5) For the purposes of this section, a person is at ***executive level***, in
4 relation to an interception agency of South Australia, if the person
5 occupies an office or position at an equivalent level to that of an
6 executive employee (within the meaning of the *Public Sector Act*
7 *2009* (SA)).

8 **317ZS Annual reports**

- 9 (1) The Minister must, as soon as practicable after each 30 June, cause
10 to be prepared a written report that sets out:
- 11 (a) the number of technical assistance requests that were given
12 during the year ending on that 30 June by the chief officers of
13 interception agencies; and
 - 14 (b) the number of technical assistance notices that were given
15 during the year ending on that 30 June by the chief officers of
16 interception agencies; and
 - 17 (c) the number of technical capability notices that were:
 - 18 (i) given during the year ending on that 30 June; and
 - 19 (ii) directed towards ensuring that designated
20 communications providers are capable of giving help to
21 interception agencies.
- 22 (2) A report under subsection (1) must be included in the report
23 prepared under subsection 186(2) of the *Telecommunications*
24 *(Interception and Access) Act 1979* relating to the year ending on
25 that 30 June.

26 **317ZT Alternative constitutional basis**

- 27 (1) Without limiting its effect apart from this section, this Part also has
28 effect as provided by this section.
- 29 (2) This Part also has the effect it would have if each reference in this
30 Part to a designated communications provider were, by express
31 provision, confined to a designated communications provider that
32 is a constitutional corporation.

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

10 Add:

11 *Concealment of access etc.*

12 (8) If any thing has been done in relation to a computer under:

13 (a) the warrant; or

14 (b) this subsection;

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

16 (c) any thing reasonably necessary to conceal the fact that any
17 thing has been done under the warrant or under this
18 subsection;

19 (d) enter any premises where the computer is reasonably
20 believed to be, for the purposes of doing the things
21 mentioned in paragraph (c);

22 (e) enter any other premises for the purposes of gaining entry to
23 or exiting the premises referred to in paragraph (d);

24 (f) remove the computer or another thing from any place where
25 it is situated for the purposes of doing the things mentioned
26 in paragraph (c), and returning the computer or other thing to
27 that place;

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

31 (i) use any other computer or a communication in transit to
32 do those things; and

33 (ii) if necessary to achieve that purpose—add, copy, delete
34 or alter other data in the computer or the communication
35 in transit;

- 1 (h) intercept a communication passing over a
2 telecommunications system, if the interception is for the
3 purposes of doing any thing mentioned in this subsection;
4 (i) any other thing reasonably incidental to any of the above;
5 at the following time:
6 (j) at any time while the warrant is in force or within 28 days
7 after it ceases to be in force;
8 (k) if none of the things mentioned in paragraph (c) are done
9 within the 28-day period mentioned in paragraph (j)—at the
10 earliest time after that 28-day period at which it is reasonably
11 practicable to do the things mentioned in paragraph (c).

12 **8 After subsection 27A(3B)**

13 Insert:

- 14 (3C) If any thing has been done in relation to a computer under:
15 (a) a warrant under this section that authorises the Organisation
16 to do acts or things referred to in subsection 25A(4); or
17 (b) this subsection;
18 the Organisation is authorised to do any of the following:
19 (c) any thing reasonably necessary to conceal the fact that any
20 thing has been done under the warrant or under this
21 subsection;
22 (d) enter any premises where the computer is reasonably
23 believed to be, for the purposes of doing the things
24 mentioned in paragraph (c);
25 (e) enter any other premises for the purposes of gaining entry to
26 or exiting the premises referred to in paragraph (d);
27 (f) remove the computer or another thing from any place where
28 it is situated for the purposes of doing the things mentioned
29 in paragraph (c), and returning the computer or other thing to
30 that place;
31 (g) if, having regard to other methods (if any) of doing the things
32 mentioned in paragraph (c) which are likely to be as
33 effective, it is reasonable in all the circumstances to do so:
34 (i) use any other computer or a communication in transit to
35 do those things; and

- 1 (ii) if necessary to achieve that purpose—add, copy, delete
2 or alter other data in the computer or the communication
3 in transit;
- 4 (h) intercept a communication passing over a
5 telecommunications system, if the interception is for the
6 purposes of doing any thing mentioned in this subsection;
- 7 (i) any other thing reasonably incidental to any of the above;
- 8 at the following time:
- 9 (j) at any time while the warrant is in force or within 28 days
10 after it ceases to be in force;
- 11 (k) if none of the things mentioned in paragraph (c) are done
12 within the 28-day period mentioned in paragraph (j)—at the
13 earliest time after that 28-day period at which it is reasonably
14 practicable to do the things mentioned in paragraph (c).

15 **9 Paragraph 27E(2)(d)**

16 Repeal the paragraph, substitute:

- 17 (d) 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) use any other computer or a communication in transit
21 for the purpose referred to in paragraph (c); and
- 22 (ii) if necessary to achieve that purpose—add, copy, delete
23 or alter other data in the computer or the communication
24 in transit;

25 **10 After paragraph 27E(2)(d)**

26 Insert:

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

30 **11 After paragraph 27E(2)(e)**

31 Insert:

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

1 **12 At the end of section 27E**

2 Add:

3 *Concealment of access etc.*

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

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

6 (b) under this subsection;

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

8 (c) any thing reasonably necessary to conceal the fact that any
9 thing has been done under the subsection (2) authorisation or
10 under this subsection;

11 (d) enter any premises where the computer is reasonably
12 believed to be, for the purposes of doing the things
13 mentioned in paragraph (c);

14 (e) enter any other premises for the purposes of gaining entry to
15 or exiting the premises referred to in paragraph (d);

16 (f) remove the computer or another thing from any place where
17 it is situated for the purposes of doing the things mentioned
18 in paragraph (c), and returning the computer or other thing to
19 that place;

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

23 (i) use any other computer or a communication in transit to
24 do those things; and

25 (ii) if necessary to achieve that purpose—add, copy, delete
26 or alter other data in the computer or the communication
27 in transit;

28 (h) intercept a communication passing over a
29 telecommunications system, if the interception is for the
30 purposes of doing any thing mentioned in this subsection;

31 (i) any other thing reasonably incidental to any of the above;

32 at the following time:

33 (j) at any time while the authorisation is in force or within 28
34 days after it ceases to be in force;

35 (k) if none of the things mentioned in paragraph (c) are done
36 within the 28-day period mentioned in paragraph (j)—at the

1 earliest time after that 28-day period at which it is reasonably
2 practicable to do the things mentioned in paragraph (c).

3 **13 Subsection 33(1)**

4 Repeal the subsection.

5 **14 Paragraph 34(2)(b)**

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

7 **15 Paragraph 34(2)(b)**

8 After “27E(2)”, insert “or (6)”.

9 **16 At the end of section 34**

10 Add:

11 (3) For the purposes of this section, any thing done under
12 subsection 25A(8) is taken to have been done under a warrant
13 issued under section 25A.

14 (4) For the purposes of this section, any thing done under
15 subsection 27A(3C) is taken to have been done under a warrant
16 issued under section 27A.

17 (5) For the purposes of this section, any thing done under
18 subsection 27E(6) is taken to have been done under a warrant
19 issued under section 27C.

20 **17 Subsection 34AA(5) (definition of *relevant authorising***
21 ***provision*)**

22 Before “26B(5)”, insert “25A(8),”.

23 **18 Subsection 34AA(5) (definition of *relevant authorising***
24 ***provision*)**

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

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

27 **25 Subsection 3(1) (definition of *protected information*)**

28 After “44(1)(a),”, insert “(aa),”.

1 **26 After Part IIIA**

2 Insert:

3 **Part IIIBB—Assistance in relation to data held in**
4 **computers**
5

6 **15CB Simplified outline of this Part**

- 7
- 8 • If a foreign country requests the Attorney-General to arrange
9 for access to data held in a computer, the Attorney-General
10 may authorise an eligible law enforcement officer to apply for
11 a computer access warrant under section 27A of the
Surveillance Devices Act 2004.
 - 12 • The authorisation relates to an investigation, or investigative
13 proceeding, relating to a criminal matter involving an offence
14 against the law of the foreign country.

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

16 **15CC Requests by foreign countries for assistance in relation to data**
17 **held in computers**

- 18 (1) The Attorney-General may, in the Attorney-General's discretion,
19 authorise an eligible law enforcement officer, in writing, to apply
20 for a computer access warrant under section 27A of the
21 *Surveillance Devices Act 2004* if the Attorney-General is satisfied
22 that:
- 23 (a) an investigation, or investigative proceeding, relating to a
24 criminal matter involving an offence against the law of a
25 foreign country (the **requesting country**) that is punishable
26 by a maximum penalty of imprisonment for 3 years or more,
27 imprisonment for life or the death penalty has commenced in
28 the requesting country; and
 - 29 (b) the requesting country requests the Attorney-General to
30 arrange for access to data held in a computer (the **target**
31 **computer**); and

- 1 (c) the requesting country has given appropriate undertakings in
2 relation to:
3 (i) ensuring that data obtained as a result of access under
4 the warrant will only be used for the purpose for which
5 it is communicated to the requesting country; 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 (2) The target computer may be any one or more of the following:
12 (a) a particular computer;
13 (b) a computer on particular premises;
14 (c) a computer associated with, used by or likely to be used by, a
15 person (whose identity may or may not be known).

- 16 (3) In this section:

17 *computer* has the same meaning as in the *Surveillance Devices Act*
18 *2004*.

19 *data* has the same meaning as in the *Surveillance Devices Act*
20 *2004*.

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

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

27 *Surveillance Devices Act 2004*

28 **27 Title**

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

30 **28 After paragraph 3(a)**

31 Insert:

- 1 (aaa) to establish procedures for law enforcement officers to obtain
2 warrants and emergency authorisations that:
3 (i) are for access to data held in computers; and
4 (ii) relate to criminal investigations and the location and
5 safe recovery of children to whom recovery orders
6 relate; and

7 **29 After paragraph 3(aa)**

8 Insert:

- 9 (aaaa) to establish procedures for law enforcement officers to obtain
10 warrants for access to data held in computers in cases where
11 a control order is in force, and access to the data would be
12 likely to substantially assist in:
13 (i) protecting the public from a terrorist act; or
14 (ii) preventing the provision of support for, or the
15 facilitation of, a terrorist act; or
16 (iii) preventing the provision of support for, or the
17 facilitation of, the engagement in a hostile activity in a
18 foreign country; or
19 (iv) determining whether the control order, or any
20 succeeding control order, has been, or is being,
21 complied with; and

22 **30 After paragraph 3(b)**

23 Insert:

- 24 (ba) to restrict the use, communication and publication of
25 information that is obtained through accessing data held in
26 computers or that is otherwise connected with computer data
27 access operations; and

28 **31 Paragraph 3(c)**

29 After “surveillance device operations”, insert “and computer data access
30 operations”.

31 **32 Subsection 4(1)**

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

33 that:

- 34 (a) prohibits or regulates the use of surveillance devices; or
-

1 (b) prohibits or regulates access to data held in computers.

2 **33 After subsection 4(4)**

3 Insert:

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

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

8 **34 After subsection 4(5)**

9 Insert:

10 (5A) For the avoidance of doubt, it is intended that a warrant may be
11 issued under this Act for access to data held in a computer in a case
12 where a control order is in force, and access to the data would be
13 likely to substantially assist in:

- 14 (a) protecting the public from a terrorist act; or
15 (b) preventing the provision of support for, or the facilitation of,
16 a terrorist act; or
17 (c) preventing the provision of support for, or the facilitation of,
18 the engagement in a hostile activity in a foreign country; or
19 (d) determining whether the control order, or any succeeding
20 control order, has been, or is being, complied with.

21 **35 Subsection 6(1)**

22 Insert:

23 *carrier* means:

- 24 (a) a carrier within the meaning of the *Telecommunications Act*
25 *1997*; or
26 (b) a carriage service provider within the meaning of that Act.

27 *communication in transit* means a communication (within the
28 meaning of the *Telecommunications Act 1997*) passing over a
29 telecommunications network (within the meaning of that Act).

30 **36 Subsection 6(1) (definition of *computer*)**

31 Repeal the definition, substitute:

- 1 **computer** means all or part of:
2 (a) one or more computers; or
3 (b) one or more computer systems; or
4 (c) one or more computer networks; or
5 (d) any combination of the above.

6 **37 Subsection 6(1)**

7 Insert:

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

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

12 **data** includes:

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

15 **data held in a computer** includes:

- 16 (a) data held in any removable data storage device for the time
17 being held in a computer; and
18 (b) data held in a data storage device on a computer network of
19 which the computer forms a part.

20 **data storage device** means a thing (for example, a disk or file
21 server) containing (whether temporarily or permanently), or
22 designed to contain (whether temporarily or permanently), data for
23 use by a computer.

24 **38 Subsection 6(1) (definition of data surveillance device)**

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

27 **39 Subsection 6(1)**

28 Insert:

29 **general computer access intercept information** has the same
30 meaning as in the *Telecommunications (Interception and Access)*
31 *Act 1979*.

1 *intercepting a communication passing over a telecommunications*
2 *system* has the same meaning as in the *Telecommunications*
3 *(Interception and Access) Act 1979*.

4 **40 Subsection 6(1) (definition of *mutual assistance***
5 ***application*)**

6 Repeal the definition, substitute:

7 *mutual assistance application* means:

8 (a) an application for a surveillance device warrant; or

9 (b) an application for a computer access warrant;

10 made under a mutual assistance authorisation.

11 **41 Subsection 6(1) (definition of *mutual assistance***
12 ***authorisation*)**

13 Omit “subsection 15CA(1)”, substitute, “subsection 15CA(1) or
14 15CC(1)”.

15 **42 Subsection 6(1) (paragraph (db) of the definition of**
16 ***relevant offence*)**

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

18 **43 Subsection 6(1) (definition of *remote application*)**

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

20 **44 Subsection 6(1)**

21 Insert:

22 *telecommunications facility* means a facility within the meaning of
23 the *Telecommunications Act 1997*.

24 **45 Subsection 6(1) (definition of *unsworn application*)**

25 Omit “or 22(4) and (5)”, substitute “, 22(4) and (5), 27A(9) and (10),
26 27A(11) and (12) or 27A(13) and (14)”.

27 **46 Subsection 6(1) (definition of *warrant*)**

28 Repeal the definition, substitute:

29 *warrant* means:

- 1 (a) a surveillance device warrant; or
2 (b) a retrieval warrant; or
3 (c) a computer access warrant.

4 **47 At the end of subsection 10(1)**

- 5 Add:
6 ; (c) a computer access warrant.

7 **48 Subsection 10(2)**

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

9 **49 At the end of Part 2**

- 10 Add:

11 **Division 4—Computer access warrants**

12 **27A Application for computer access warrant**

13 *Warrants sought for offence investigations*

- 14 (1) A law enforcement officer (or another person on the law
15 enforcement officer’s behalf) may apply for the issue of a
16 computer access warrant if the law enforcement officer suspects on
17 reasonable grounds that:
18 (a) one or more relevant offences have been, are being, are about
19 to be, or are likely to be, committed; and
20 (b) an investigation into those offences is being, will be, or is
21 likely to be, conducted; and
22 (c) access to data held in a computer (the *target computer*) is
23 necessary, in the course of that investigation, for the purpose
24 of enabling evidence to be obtained of:
25 (i) the commission of those offences; or
26 (ii) the identity or location of the offenders.
- 27 (2) If the application is being made by or on behalf of a State or
28 Territory law enforcement officer, the reference in subsection (1)
29 to a relevant offence does not include a reference to a State offence
30 that has a federal aspect.

1 by enabling evidence to be obtained relating to the integrity,
2 location or identity of any staff member of the target agency.

3 *Control order access warrants*

- 4 (6) 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:
7 (a) a control order is in force in relation to a person; and
8 (b) the law enforcement officer suspects on reasonable grounds
9 that access to data held in a computer (the **target computer**)
10 to obtain information relating to the person would be likely to
11 substantially assist in:
12 (i) protecting the public from a terrorist act; or
13 (ii) preventing the provision of support for, or the
14 facilitation of, a terrorist act; or
15 (iii) preventing the provision of support for, or the
16 facilitation of, the engagement in a hostile activity in a
17 foreign country; or
18 (iv) determining whether the control order, or any
19 succeeding control order, has been, or is being,
20 complied with.

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

23 *Procedure for making applications*

- 24 (7) An application under subsection (1), (3), (4), (5) or (6) may be
25 made to an eligible Judge or to a nominated AAT member.
- 26 (8) An application:
27 (a) must specify:
28 (i) the name of the applicant; and
29 (ii) the nature and duration of the warrant sought; and
30 (b) subject to this section, must be supported by an affidavit
31 setting out the grounds on which the warrant is sought.

32 *Unsworn applications—warrants sought for offence investigations*

- 33 (9) If a law enforcement officer believes that:
-

- 1 (a) immediate access to data held in the target computer referred
2 to in subsection (1) is necessary as described in
3 paragraph (1)(c); and
4 (b) it is impracticable for an affidavit to be prepared or sworn
5 before an application for a warrant is made;
6 an application for a warrant under subsection (1) may be made
7 before an affidavit is prepared or sworn.

- 8 (10) If subsection (9) applies, the applicant must:
9 (a) provide as much information as the eligible Judge or
10 nominated AAT member considers is reasonably practicable
11 in the circumstances; and
12 (b) not later than 72 hours after the making of the application,
13 send a duly sworn affidavit to the eligible Judge or
14 nominated AAT member, whether or not a warrant has been
15 issued.

16 *Unsworn applications—warrants sought for recovery orders*

- 17 (11) If a law enforcement officer believes that:
18 (a) immediate access to data held in the target computer referred
19 to in subsection (3) may assist as described in
20 paragraph (3)(b); and
21 (b) it is impracticable for an affidavit to be prepared or sworn
22 before an application for a warrant is made;
23 an application for a warrant under subsection (3) may be made
24 before an affidavit is prepared or sworn.

- 25 (12) If subsection (11) applies, the applicant must:
26 (a) provide as much information as the eligible Judge or
27 nominated AAT member considers is reasonably practicable
28 in the circumstances; and
29 (b) not later than 72 hours after the making of the application,
30 send a duly sworn affidavit to the eligible Judge or
31 nominated AAT member, whether or not a warrant has been
32 issued.

33 *Unsworn applications—control order access warrants*

- 34 (13) If a law enforcement officer believes that:
-

- 1 (a) immediate access to data held in the target computer referred
2 to in subsection (6) would be likely to substantially assist as
3 described in paragraph (6)(b); and
4 (b) it is impracticable for an affidavit to be prepared or sworn
5 before an application for a warrant is made;
6 an application for a warrant under subsection (6) may be made
7 before an affidavit is prepared or sworn.

- 8 (14) If subsection (13) applies, the applicant must:
9 (a) provide as much information as the eligible Judge or
10 nominated AAT member considers is reasonably practicable
11 in the circumstances; and
12 (b) not later than 72 hours after the making of the application,
13 send a duly sworn affidavit to the eligible Judge or
14 nominated AAT member, whether or not a warrant has been
15 issued.

16 *Target computer*

- 17 (15) The target computer referred to in subsection (1), (3), (4), (5) or (6)
18 may be any one or more of the following:
19 (a) a particular computer;
20 (b) a computer on particular premises;
21 (c) a computer associated with, used by or likely to be used by, a
22 person (whose identity may or may not be known).

23 **27B Remote application**

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

1 **27C Determining the application**

2 (1) An eligible Judge or a nominated AAT member may issue a
3 computer access warrant if satisfied:

4 (a) in the case of a warrant sought in relation to a relevant
5 offence—that there are reasonable grounds for the suspicion
6 founding the application for the warrant; and

7 (b) in the case of a warrant sought in relation to a recovery
8 order—that such an order is in force and that there are
9 reasonable grounds for the suspicion founding the application
10 for the warrant; and

11 (c) in the case of a warrant sought in relation to a mutual
12 assistance authorisation—that such an authorisation is in
13 force and that there are reasonable grounds for the suspicion
14 founding the application for the warrant; and

15 (d) in the case of a warrant sought for the purposes of an
16 integrity operation—that the integrity authority for the
17 operation is in effect, and that there are reasonable grounds
18 for the suspicions founding the application for the warrant (as
19 mentioned in paragraphs 27A(5)(a) and (b)); and

20 (e) in the case of a control order access warrant—that a control
21 order is in force in relation to a person, and that access to
22 data held in the relevant target computer to obtain
23 information relating to the person would be likely to
24 substantially 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 (f) in the case of an unsworn application—that it would have
35 been impracticable for an affidavit to have been sworn or
36 prepared before the application was made; and

1 (g) in the case of a remote application—that it would have been
2 impracticable for the application to have been made in
3 person.

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

6 (2) In determining whether a computer access warrant should be
7 issued, the eligible Judge or nominated AAT member must have
8 regard to:

9 (a) in the case of a warrant sought in relation to a relevant
10 offence or a mutual assistance authorisation, or for the
11 purposes of an integrity operation—the nature and gravity of
12 the alleged offence; and

13 (b) in the case of a warrant sought to assist in the location and
14 safe recovery of a child to whom a recovery order relates—
15 the circumstances that gave rise to the making of the order;
16 and

17 (c) the extent to which the privacy of any person is likely to be
18 affected; and

19 (d) the existence of any alternative means of obtaining the
20 evidence or information sought to be obtained; and

21 (e) in the case of a warrant sought in relation to a relevant
22 offence or a recovery order, or for the purposes of an
23 integrity operation—the likely evidentiary or intelligence
24 value of any evidence or information sought to be obtained;
25 and

26 (f) in the case of a warrant sought in relation to a mutual
27 assistance authorisation—the likely evidentiary or
28 intelligence value of any evidence or information sought to
29 be obtained, to the extent that this is possible to determine
30 from information obtained from the foreign country to which
31 the authorisation relates; and

32 (g) in the case of a control order access warrant issued on the
33 basis of a control order that is in force in relation to a
34 person—the likely value of the information sought to be
35 obtained, in:

36 (i) protecting the public from a terrorist act; or

37 (ii) preventing the provision of support for, or the
38 facilitation of, a terrorist act; or

Schedule 2 Computer access warrants etc.

Part 1 Amendments

- 1 (iii) preventing the provision of support for, or the
2 facilitation of, the engagement in a hostile activity in a
3 foreign country; or
4 (iv) determining whether the control order, or any
5 succeeding control order, has been, or is being,
6 complied with; and
7 (h) in the case of a control order access warrant issued on the
8 basis of a control order that is in force in relation to a
9 person—whether the access to data held in the relevant target
10 computer in accordance with the warrant would be the means
11 of obtaining the evidence or information sought to be
12 obtained, that is likely to have the least interference with any
13 person’s privacy; and
14 (i) in the case of a control order access warrant issued on the
15 basis of a control order that is in force in relation to a
16 person—the possibility that the person:
17 (i) has engaged, is engaging, or will engage, in a terrorist
18 act; or
19 (ii) has provided, is providing, or will provide, support for a
20 terrorist act; or
21 (iii) has facilitated, is facilitating, or will facilitate, a terrorist
22 act; or
23 (iv) has provided, is providing, or will provide, support for
24 the engagement in a hostile activity in a foreign country;
25 or
26 (v) has facilitated, is facilitating, or will facilitate, the
27 engagement in a hostile activity in a foreign country; or
28 (vi) has contravened, is contravening, or will contravene, the
29 control order; or
30 (vii) will contravene a succeeding control order; and
31 (j) in the case of a warrant sought in relation to a relevant
32 offence or a recovery order—any previous warrant sought or
33 issued under this Division in connection with the same
34 alleged offence or the same recovery order; and
35 (k) in the case of a control order access warrant issued on the
36 basis of a control order that is in force in relation to a
37 person—any previous control order access warrant sought or
38 issued on the basis of a control order relating to the person.
-

1 **27D What must a computer access warrant contain?**

2 (1) A computer access warrant must:

3 (a) state that the eligible Judge or nominated AAT member
4 issuing the warrant is satisfied of the matters referred to in
5 subsection 27C(1) and has had regard to the matters referred
6 to in subsection 27C(2); and

7 (b) specify:

8 (i) the name of the applicant; and

9 (ii) if the warrant relates to one or more alleged relevant
10 offences—the alleged offences in respect of which the
11 warrant is issued; and

12 (iii) if the warrant relates to a recovery order—the date the
13 order was made and the name of the child to whom the
14 order relates; and

15 (iv) if the warrant relates to a mutual assistance
16 authorisation—the offence or offences against the law
17 of a foreign country to which the authorisation relates;
18 and

19 (v) if the warrant is issued for the purposes of an integrity
20 operation—the integrity authority for the operation and
21 each alleged relevant offence in relation to which the
22 authority was granted; and

23 (vi) the date the warrant is issued; and

24 (vii) if the target computer is or includes a particular
25 computer—the computer; and

26 (viii) if the target computer is or includes a computer on
27 particular premises—the premises; and

28 (ix) if the target computer is or includes a computer
29 associated with, used by or likely to be used by, a
30 person—the person (whether by name or otherwise);
31 and

32 (x) the period during which the warrant is in force (see
33 subsection (3)); and

34 (xi) the name of the law enforcement officer primarily
35 responsible for executing the warrant.

- 1 (2) If a control order access warrant is issued on the basis of a control
2 order that is in force in relation to a person, the warrant must also
3 specify the following details in relation to the control order:
4 (a) the name of the person;
5 (b) the date the control order was made;
6 (c) whether the control order is an interim control order or a
7 confirmed control order.
- 8 (3) A warrant may only be issued:
9 (a) for a period of no more than 90 days; or
10 (b) if the warrant is issued for the purposes of an integrity
11 operation—for a period of no more than 21 days.
- 12 Note: The access to data held in the target computer pursuant to a warrant
13 may be discontinued earlier—see section 27H.
- 14 (4) In the case of a warrant authorising the access to data held in the
15 target computer on premises that are vehicles, the warrant need
16 only specify the class of vehicle in relation to which the access to
17 data held in the target computer is authorised.
- 18 (5) A warrant must be signed by the person issuing it and include the
19 person's name.
- 20 (6) As soon as practicable after completing and signing a warrant
21 issued on a remote application, the person issuing it must:
22 (a) inform the applicant of:
23 (i) the terms of the warrant; and
24 (ii) the date on which, and the time at which, the warrant
25 was issued; and
26 (b) give the warrant to the applicant while retaining a copy of the
27 warrant for the person's own record.

28 **27E What a computer access warrant authorises**

- 29 (1) A computer access warrant must authorise the doing of specified
30 things (subject to any restrictions or conditions specified in the
31 warrant) in relation to the relevant target computer.

- 1 (2) The things that may be specified are any of the following that the
2 eligible Judge or nominated AAT member considers appropriate in
3 the circumstances:
- 4 (a) entering specified premises for the purposes of doing the
5 things mentioned in this subsection;
- 6 (b) entering any premises for the purposes of gaining entry to, or
7 exiting, the specified premises;
- 8 (c) using:
- 9 (i) the target computer; 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 target computer at any time while the
16 warrant is in force, in order to determine whether the relevant
17 data is covered by the warrant;
- 18 (d) if necessary to achieve the purpose mentioned in
19 paragraph (c)—adding, copying, deleting or altering other
20 data in the target computer;
- 21 (e) if, having regard to other methods (if any) of obtaining access
22 to the relevant data which are likely to be as effective, it is
23 reasonable in all the circumstances to do so:
- 24 (i) using any other computer or a communication in transit
25 to access the relevant data; and
26 (ii) if necessary to achieve that purpose—adding, copying,
27 deleting or altering other data in the computer or the
28 communication in transit;
- 29 (f) removing a computer or other thing from premises for the
30 purposes of doing any thing specified in the warrant in
31 accordance with this subsection, and returning the computer
32 or other thing to the premises;
- 33 (g) copying any data to which access has been obtained, and that:
- 34 (i) appears to be relevant for the purposes of determining
35 whether the relevant data is covered by the warrant; or
36 (ii) is covered by the warrant;
- 37 (h) intercepting a communication passing over a
38 telecommunications system, if the interception is for the
-

- 1 purposes of doing any thing specified in the warrant in
2 accordance with this subsection;
3 (i) any other thing reasonably incidental to any of the above.

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

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

14 *When data is covered by a warrant*

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

31 *Certain acts not authorised*

- 32 (5) Subsection (2) does not authorise the addition, deletion or
33 alteration of data, or the doing of any thing, that is likely to:
34 (a) materially interfere with, interrupt or obstruct:
35 (i) a communication in transit; or

- 1 (ii) the lawful use by other persons of a computer;
2 unless the addition, deletion or alteration, or the doing of the
3 thing, is necessary to do one or more of the things specified
4 in the warrant; or
5 (b) cause any other material loss or damage to other persons
6 lawfully using a computer.

7 *Warrant must provide for certain matters*

- 8 (6) A computer access warrant must:
9 (a) authorise the use of any force against persons and things that
10 is necessary and reasonable to do the things specified in the
11 warrant; and
12 (b) if the warrant authorises entering premises—state whether
13 entry is authorised to be made at any time of the day or night
14 or during stated hours of the day or night.

15 *Concealment of access etc.*

- 16 (7) If any thing has been done in relation to a computer under:
17 (a) a computer access warrant; or
18 (b) this subsection;
19 then, in addition to the things specified in the warrant, the warrant
20 authorises the doing of any of the following:
21 (c) any thing reasonably necessary to conceal the fact that any
22 thing has been done under the warrant or under this
23 subsection;
24 (d) entering any premises where the computer is reasonably
25 believed to be, for the purposes of doing the things
26 mentioned in paragraph (c);
27 (e) entering any other premises for the purposes of gaining entry
28 to or exiting the premises referred to in paragraph (d);
29 (f) removing the computer or another thing from any place
30 where it is situated for the purposes of doing the things
31 mentioned in paragraph (c), and returning the computer or
32 other thing to that place;
33 (g) if, having regard to other methods (if any) of doing the things
34 mentioned in paragraph (c) which are likely to be as
35 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 **27F Extension and variation of computer access warrant**

- 18 (1) A law enforcement officer to whom a computer access warrant has
19 been issued (or another person on the law enforcement officer's
20 behalf) may apply, at any time before the expiry of the warrant:
21 (a) for an extension of the warrant for a period of no more than:
22 (i) 90 days after the day the warrant would otherwise
23 expire; or
24 (ii) if the warrant is issued for the purposes of an integrity
25 operation—21 days after the day the warrant would
26 otherwise expire; or
27 (b) for a variation of any of the other terms of the warrant.
- 28 (2) The application is to be made to an eligible Judge or to a
29 nominated AAT member and must be accompanied by the original
30 warrant.
- 31 (3) Sections 27A and 27B apply, with any necessary changes, to an
32 application under this section as if it were an application for the
33 warrant.
- 34 (4) The eligible Judge or nominated AAT member may grant an
35 application if satisfied that the matters referred to in

1 subsection 27C(1) still exist, having regard to the matters in
2 subsection 27C(2).

3 (5) If the eligible Judge or nominated AAT member grants the
4 application, the eligible Judge or nominated AAT member must
5 endorse the new expiry date or the other varied term on the original
6 warrant.

7 (6) An application may be made under this section more than once.

8 **27G Revocation of computer access warrant**

9 (1) A computer access warrant may, by instrument in writing, be
10 revoked by an eligible Judge or nominated AAT member on the
11 initiative of the eligible Judge or nominated AAT member at any
12 time before the expiration of the period of validity specified in the
13 warrant.

14 (2) If the circumstances set out in paragraphs 27H(2)(a) and (b),
15 27H(3)(a) and (b), 27H(4)(a) and (b), 27H(5)(a) and (b), 27H(6)(a)
16 and (b) or 27H(7)(a) and (b) apply in relation to a computer access
17 warrant, the chief officer of the law enforcement agency to which
18 the law enforcement officer to whom the warrant was issued
19 belongs or is seconded must, by instrument in writing, revoke the
20 warrant.

21 (3) The instrument revoking a warrant must be signed by the eligible
22 Judge, the nominated AAT member or the chief officer of the law
23 enforcement agency, as the case requires.

24 (4) If an eligible Judge or nominated AAT member revokes a warrant,
25 the eligible Judge or nominated AAT member must give a copy of
26 the instrument of revocation to the chief officer of the law
27 enforcement agency to which the law enforcement officer to whom
28 the warrant was issued belongs or is seconded.

29 (5) If:

30 (a) an eligible Judge or nominated AAT member revokes a
31 warrant; and

32 (b) at the time of the revocation, a law enforcement officer is
33 executing the warrant;

1 the law enforcement officer is not subject to any civil or criminal
2 liability for any act done in the proper execution of that warrant
3 before the officer is made aware of the revocation.

4 **27H Discontinuance of access under warrant**

5 *Scope*

6 (1) This section applies if a computer access warrant is issued to a law
7 enforcement officer.

8 *Discontinuance of access*

9 (2) If:

- 10 (a) the computer access warrant has been sought by or on behalf
11 of a law enforcement officer in relation to a relevant offence;
12 and
13 (b) the chief officer of the law enforcement agency to which the
14 law enforcement officer belongs or is seconded is satisfied
15 that access to data under the warrant is no longer required for
16 the purpose of enabling evidence to be obtained of:
17 (i) the commission of the relevant offence; or
18 (ii) the identity or location of the offender;

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

22 (3) If:

- 23 (a) the computer access warrant has been sought by or on behalf
24 of a law enforcement officer in relation to a recovery order;
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 locating and safely recovering the child to
30 whom the recovery order relates;

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

- 1 (4) If:
2 (a) the computer access warrant has been sought by or on behalf
3 of a law enforcement officer as authorised under a mutual
4 assistance authorisation; and
5 (b) the chief officer of the law enforcement agency to which the
6 law enforcement officer belongs or is seconded is satisfied
7 that access to data under the warrant is no longer required for
8 the purpose of enabling evidence to be obtained of:
9 (i) the commission of the offence against a law of a foreign
10 country to which the authorisation relates; or
11 (ii) the identity or location of the persons suspected of
12 committing the offence;
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 (5) If:
17 (a) the computer access warrant has been sought by or on behalf
18 of a federal law enforcement officer for the purposes of an
19 integrity operation; 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:
23 (i) access to data under the warrant is no longer necessary
24 for the purposes of the integrity operation; or
25 (ii) the integrity authority for the integrity operation is no
26 longer in effect;
27 the chief officer must, in addition to revoking the warrant under
28 section 27G, take the steps necessary to ensure access to data
29 authorised by the warrant is discontinued.
- 30 (6) If:
31 (a) the computer access warrant is a control order access warrant
32 issued on the basis of a control order that was in force in
33 relation to a person; and
34 (b) the chief officer of the law enforcement agency to which the
35 law enforcement officer belongs or is seconded is satisfied
36 that access to data under the warrant to obtain information

- 1 relating to the person is no longer required for any of the
2 following purposes:
- 3 (i) protecting the public from a terrorist act;
 - 4 (ii) preventing the provision of support for, or the
5 facilitation of, a terrorist act;
 - 6 (iii) preventing the provision of support for, or the
7 facilitation of, the engagement in a hostile activity in a
8 foreign country;
 - 9 (iv) determining whether the control order, or any
10 succeeding control order, has been, or is being,
11 complied with;

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

15 (7) If:

16 (a) the computer access warrant is a control order access warrant
17 issued on the basis of a control order that was in force in
18 relation to a person; and

19 (b) no control order is in force in relation to the person;

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

23 (8) If the chief officer of a law enforcement agency is notified that a
24 warrant has been revoked by an eligible Judge or a nominated
25 AAT member under section 27G, the eligible Judge or nominated
26 AAT member must take the steps necessary to ensure that access to
27 data authorised by the warrant is discontinued as soon as
28 practicable.

29 (9) If the law enforcement officer to whom the warrant is issued, or
30 who is primarily responsible for executing the warrant, believes
31 that access to data under the warrant is no longer necessary for the
32 purpose:

33 (a) if the warrant was issued in relation to a relevant offence—of
34 enabling evidence to be obtained of the commission of the
35 relevant offence or the identity or location of the offender; or

- 1 (b) if the warrant was issued in relation to a recovery order—of
2 enabling the location and safe recovery of the child to whom
3 the order relates; or
4 (c) if the warrant was issued in relation to a mutual assistance
5 authorisation—of enabling evidence to be obtained of:
6 (i) the commission of the offence against a law of a foreign
7 country to which the authorisation relates; or
8 (ii) the identity or location of the persons suspected of
9 committing the offence;
10 the law enforcement officer must immediately inform the chief
11 officer of the law enforcement agency to which the law
12 enforcement officer belongs or is seconded.
- 13 (10) In the case of a warrant issued for the purposes of an integrity
14 operation, if the law enforcement officer to whom the warrant is
15 issued, or who is primarily responsible for executing the warrant,
16 believes that:
17 (a) access to data under the warrant is no longer necessary for
18 those purposes; or
19 (b) the integrity authority for the integrity operation is no longer
20 in effect;
21 the law enforcement officer must immediately inform the chief
22 officer of the law enforcement agency to which the law
23 enforcement officer belongs or is seconded.

24 **50 After subsection 28(1)**

25 Insert:

- 26 (1A) A law enforcement officer may apply to an appropriate authorising
27 officer for an emergency authorisation for access to data held in a
28 computer (the *target computer*) if, in the course of an investigation
29 of a relevant offence, the law enforcement officer reasonably
30 suspects that:
31 (a) an imminent risk of serious violence to a person or
32 substantial damage to property exists; and
33 (b) access to data held in the target computer is immediately
34 necessary for the purpose of dealing with that risk; and

1 (c) the circumstances are so serious and the matter is of such
2 urgency that access to data held in the target computer is
3 warranted; and

4 (d) it is not practicable in the circumstances to apply for a
5 computer access warrant.

6 (1B) The target computer may be any one or more of the following:

7 (a) a particular computer;

8 (b) a computer on particular premises;

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

11 **51 Subsections 28(2), (3) and (4)**

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

13 **52 After subsection 29(1)**

14 Insert:

15 (1A) A law enforcement officer may apply to an appropriate authorising
16 officer for an emergency authorisation for access to data held in a
17 computer (the *target computer*) if:

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

19 (b) the law enforcement officer reasonably suspects that:

20 (i) the circumstances are so urgent as to warrant immediate
21 access to data held in the target computer; and

22 (ii) it is not practicable in the circumstances to apply for a
23 computer access warrant.

24 (1B) The target computer may be any one or more of the following:

25 (a) a particular computer;

26 (b) a computer on particular premises;

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

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

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

31 **54 After subsection 30(1)**

32 Insert:

- 1 (1A) If:
2 (a) a law enforcement officer is conducting an investigation into:
3 (i) an offence against section 233BAA of the *Customs Act*
4 *1901* (with respect to goods listed in Schedule 4 to the
5 *Customs (Prohibited Imports) Regulations 1956* or in
6 Schedule 8 or 9 to the *Customs (Prohibited Exports)*
7 *Regulations 1958*); or
8 (ii) an offence under the *Crimes (Traffic in Narcotic Drugs*
9 *and Psychotropic Substances) Act 1990* or an offence
10 against Part 9.1 of the *Criminal Code* (other than
11 section 308.1 or 308.2); or
12 (iii) an offence against section 73.2 or 73.3 or Division 91 of
13 the *Criminal Code*; or
14 (iv) an offence under Subdivision A of Division 72 or
15 Division 80, 101, 102, 103, 270, 272 or 273 of the
16 *Criminal Code*; or
17 (v) an offence against section 233B or 233C of the
18 *Migration Act 1958*;
19 or more than one offence; and
20 (b) the law enforcement officer reasonably suspects that:
21 (i) access to data held in a computer (the **target computer**)
22 is immediately necessary to prevent the loss of any
23 evidence relevant to that investigation; and
24 (ii) the circumstances are so serious and the matter is of
25 such urgency that access to data held in the target
26 computer is warranted; and
27 (iii) it is not practicable in the circumstances to apply for a
28 computer access warrant;
29 the law enforcement officer may apply to an appropriate
30 authorising officer for an emergency authorisation for access to
31 data held in the target computer.
- 32 (1B) The target computer may be any one or more of the following:
33 (a) a particular computer;
34 (b) a computer on particular premises;
35 (c) a computer associated with, used by or likely to be used by, a
36 person (whose identity may or may not be known).

1 **55 Subsection 30(2)**

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

3 **56 Subsection 30(3)**

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

6 **57 At the end of section 30**

7 Add:

8 (4) In the case of an application mentioned in subsection (1A), the
9 appropriate authorising officer may give the emergency
10 authorisation if satisfied that:

11 (a) an investigation is being conducted into an offence referred
12 to in paragraph (1A)(a); and

13 (b) there are reasonable grounds for the suspicion referred to in
14 paragraph (1A)(b).

15 **58 Subsections 32(1) and (2)**

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

17 **59 After subsection 32(2)**

18 Insert:

19 (2A) An emergency authorisation for access to data held in a computer
20 may authorise anything that a computer access warrant may
21 authorise.

22 **60 After subsection 32(3)**

23 Insert:

24 (3A) A law enforcement officer may, under an emergency authorisation,
25 access data held in a computer only if the officer is acting in the
26 performance of the officer’s duty.

27 **61 Subsection 33(2)**

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

1 **62 After subsection 33(2)**

2 Insert:

3 (2A) In the case of an application for an emergency authorisation for
4 access to data held in a computer, the application:

5 (a) must specify:

6 (i) the name of the applicant for the approval; and

7 (ii) if a warrant is sought—the nature and duration of the
8 warrant; and

9 (b) must be supported by an affidavit setting out the grounds on
10 which the approval (and warrant, if any) is sought; and

11 (c) must be accompanied by a copy of the written record made
12 under section 31 in relation to the emergency authorisation.

13 **63 Subsection 34(1)**

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

15 **64 After subsection 34(1)**

16 Insert:

17 (1A) Before deciding an application for approval of the giving of an
18 emergency authorisation given in response to an application under
19 subsection 28(1A), the eligible Judge or nominated AAT member
20 considering the application must, in particular, and being mindful
21 of the intrusive nature of accessing data held in the target computer
22 mentioned in that subsection, consider the following:

23 (a) the nature of the risk of serious violence to a person or
24 substantial damage to property;

25 (b) the extent to which issuing a computer access warrant would
26 have helped reduce or avoid the risk;

27 (c) the extent to which law enforcement officers could have used
28 alternative methods of investigation to help reduce or avoid
29 the risk;

30 (d) how much the use of alternative methods of investigation
31 could have helped reduce or avoid the risk;

32 (e) how much the use of alternative methods of investigation
33 would have prejudiced the safety of the person or property
34 because of delay or for another reason;

- 1 (f) whether or not it was practicable in the circumstances to
2 apply for a computer access warrant.

3 **65 Subsection 34(2)**

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

5 **66 After subsection 34(2)**

6 Insert:

- 7 (2A) Before deciding an application for approval of the giving of an
8 emergency authorisation given in response to an application under
9 subsection 29(1A), the eligible Judge or nominated AAT member
10 considering the application must, in particular, and being mindful
11 of the intrusive nature of accessing data held in the target computer
12 mentioned in that subsection, consider the following:
- 13 (a) the urgency of enforcing the recovery order;
 - 14 (b) the extent to which access to data held in the target computer
15 mentioned in that subsection would assist in the location and
16 safe recovery of the child to whom the recovery order relates;
 - 17 (c) the extent to which law enforcement officers could have used
18 alternative methods to assist in the location and safe recovery
19 of the child;
 - 20 (d) how much the use of alternative methods to assist in the
21 location and safe recovery of the child might have prejudiced
22 the effective enforcement of the recovery order;
 - 23 (e) whether or not it was practicable in the circumstances to
24 apply for a computer access warrant.

25 **67 Subsection 34(3)**

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

27 **68 At the end of section 34**

28 Add:

- 29 (4) Before deciding an application for approval of the giving of an
30 emergency authorisation given in response to an application under
31 subsection 30(1A), the eligible Judge or nominated AAT member
32 must, in particular, and being mindful of the intrusive nature of

- 1 accessing data held in the target computer mentioned in that
2 subsection, consider the following:
- 3 (a) the nature of the risk of the loss of evidence;
 - 4 (b) the extent to which issuing a computer access warrant would
5 have helped reduce or avoid the risk;
 - 6 (c) the extent to which law enforcement officers could have used
7 alternative methods of investigation to help reduce or avoid
8 the risk;
 - 9 (d) how much the use of alternative methods of investigation
10 could have helped reduce or avoid the risk;
 - 11 (e) whether or not it was practicable in the circumstances to
12 apply for a computer access warrant.

13 **69 Section 35 (heading)**

14 Repeal the heading, substitute:

15 **35 Judge or nominated AAT member may approve giving of an**
16 **emergency authorisation for the use of a surveillance**
17 **device**

18 **70 Subsection 35(1)**

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

21 **71 Subsection 35(1)**

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

23 **72 Subsection 35(2)**

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

26 **73 Subsection 35(2)**

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

28 **74 Subsection 35(3)**

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

1 **75 Subsection 35(3)**

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

3 **76 After section 35**

4 Insert:

5 **35A Judge or nominated AAT member may approve giving of an**
6 **emergency authorisation for access to data held in a**
7 **computer**

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

- 1 (3) After considering an application for approval of the giving of an
2 emergency authorisation in response to an application under
3 subsection 30(1A), the eligible Judge or nominated AAT member
4 may give the approval if satisfied that:
- 5 (a) there were reasonable grounds to suspect that:
6 (i) there was a risk of loss of evidence; and
7 (ii) accessing data held in the target computer mentioned in
8 that subsection may have helped reduce the risk; and
9 (b) it was not practicable in the circumstances to apply for a
10 computer access warrant.
- 11 (4) If, under subsection (1), (2) or (3), the eligible Judge or nominated
12 AAT member approves the giving of an emergency authorisation,
13 the eligible Judge or nominated AAT member may:
- 14 (a) unless paragraph (b) applies—issue a computer access
15 warrant relating to the continued access to data held in the
16 relevant target computer as if the application for the approval
17 were an application for a computer access warrant under
18 Division 4 of Part 2; or
19 (b) if the eligible Judge or nominated AAT member is satisfied
20 that, since the application for the emergency authorisation,
21 the activity that required access to data held in the relevant
22 target computer has ceased—order that access to data held in
23 that computer cease.
- 24 (5) If, under subsection (1), (2) or (3), the eligible Judge or nominated
25 AAT member does not approve the giving of an emergency
26 authorisation, the eligible Judge or nominated AAT member may:
- 27 (a) order that access to data held in the relevant target computer
28 cease; or
29 (b) if the eligible Judge or nominated AAT member is of the
30 view that, although the situation did not warrant the
31 emergency authorisation at the time that authorisation was
32 given, the use of a computer access warrant under Division 4
33 of Part 2 is currently justified—issue a computer access
34 warrant relating to the subsequent access to such data as if
35 the application for the approval were an application for a
36 computer access warrant under Division 4 of Part 2.

- 1 (6) In any case, the eligible Judge or nominated AAT member may
2 order that any information obtained from or relating to the exercise
3 of powers under the emergency authorisation, or any record of that
4 information, be dealt with in a manner specified in the order, so
5 long as the manner does not involve the destruction of that
6 information.

7 **77 Section 36**

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

9 **78 Section 41 (definition of *appropriate consenting official*)**

10 Repeal the definition, substitute:

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

- 12 (a) when used in section 42 or 43—means an official of that
13 country having authority in that country to give consent to
14 the use of surveillance devices in that country or on a vessel
15 or aircraft registered under the laws of that country; or
16 (b) when used in section 43A or 43B—means an official of that
17 country having authority in that country to give consent to
18 access to data held in computers in that country or on a vessel
19 or aircraft registered under the laws of that country.

20 **79 Section 42 (heading)**

21 Repeal the heading, substitute:

22 **42 Extraterritorial operation of surveillance device warrants**

23 **80 Subsection 42(1)**

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

25 **81 After paragraph 42(2)(a)**

26 Insert:

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

29 **82 Paragraph 42(2)(b)**

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

1 **83 Subsection 42(2)**

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

3 **84 Subsection 42(2)**

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

5 **85 Paragraph 42(3)(a)**

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

7 **86 Subsections 42(6) and (9)**

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

9 **87 At the end of Part 5**

10 Add:

11 **43A Extraterritorial operation of computer access warrants**

12 (1) If, before the issue of a computer access warrant in relation to the
13 investigation of a relevant offence in response to an application
14 made by or on behalf of a federal law enforcement officer, it
15 becomes apparent to the applicant that there will be a need for
16 access to data held in a computer:

17 (a) in a foreign country; or

18 (b) on a vessel or aircraft that is registered under the law of a
19 foreign country and is in or above waters beyond the outer
20 limits of the territorial sea of Australia;

21 to assist in that investigation, the eligible Judge or nominated AAT
22 member considering the application for the warrant must not
23 permit the warrant to authorise that access unless the eligible Judge
24 or nominated AAT member is satisfied that the access has been
25 agreed to by an appropriate consenting official of the foreign
26 country.

27 (2) If:

28 (a) application is made under section 33 by an appropriate
29 authorising officer who is a federal law enforcement officer
30 for approval of the giving of an emergency authorisation
31 relating to the investigation of a relevant offence; and

- 1 (b) the emergency authorisation was given in response to an
2 application under subsection 28(1A); and
- 3 (c) before the completion of consideration of that section 33
4 application, it becomes apparent to the applicant that there
5 will be a need for access to data held in a computer:
- 6 (i) in a foreign country; or
7 (ii) on a vessel or aircraft that is registered under the law of
8 a foreign country and is in or above waters beyond the
9 outer limits of the territorial sea of Australia;
- 10 to assist in the investigation to which the emergency
11 authorisation related;
- 12 the eligible Judge or nominated AAT member to whom the
13 section 33 application was made must not permit any computer
14 access warrant issued on consideration of that section 33
15 application to authorise that access unless the eligible Judge or
16 nominated AAT member is satisfied that the access has been
17 agreed to by an appropriate consenting official of the foreign
18 country.
- 19 (3) If:
- 20 (a) a computer access warrant has been issued in relation to the
21 investigation of a relevant offence in response to an
22 application by or on behalf of a federal law enforcement
23 officer; and
- 24 (b) after the issue of the warrant, it becomes apparent to the law
25 enforcement officer primarily responsible for executing the
26 warrant that there will be a need for access to data held in a
27 computer that is:
- 28 (i) in a foreign country; or
29 (ii) on a vessel or aircraft that is registered under the law of
30 a foreign country and is in or above waters beyond the
31 outer limits of the territorial sea of Australia;
- 32 to assist in that investigation;
- 33 the warrant is taken to permit that access if, and only if, the access
34 has been agreed to by an appropriate consenting official of the
35 foreign country.
- 36 (4) Subsections (1), (2) and (3) do not apply to a computer access
37 warrant authorising access to data if:
-

- 1 (a) the person, or each of the persons, responsible for executing
2 the warrant will be physically present in Australia; and
3 (b) the location where the data is held is unknown or cannot
4 reasonably be determined.
- 5 (5) Despite subsections (1), (2) and (3), if:
6 (a) a vessel that is registered under the law of a foreign country
7 is in waters beyond the outer limits of the territorial sea of
8 Australia but not beyond the outer limits of the contiguous
9 zone of Australia; and
10 (b) the relevant offence in respect of which it becomes apparent
11 that access to data held in a computer on the vessel will be
12 required is an offence relating to the customs, fiscal,
13 immigration or sanitary laws of Australia;
14 there is no requirement for the agreement of an appropriate
15 consenting official of the foreign country concerned in relation to
16 that access while the vessel is in such waters.
- 17 (6) Despite subsections (1), (2) and (3), if:
18 (a) a vessel that is registered under the law of a foreign country
19 is in waters beyond the outer limits of the territorial sea of
20 Australia but not beyond the outer limits of the Australian
21 fishing zone; and
22 (b) the relevant offence in respect of which it becomes apparent
23 that access to data held in a computer on the vessel will be
24 required is an offence against section 100, 100A, 100B, 101,
25 101A or 101AA of the *Fisheries Management Act 1991* or
26 section 46A, 46B, 46C, 46D, 49A or 51A of the *Torres Strait*
27 *Fisheries Act 1984*;
28 there is no requirement for the agreement of an appropriate
29 consenting official of the foreign country concerned in relation to
30 that access while the vessel is in those waters.
- 31 (7) As soon as practicable after the commencement of access to data
32 held in a computer under the authority of a computer access
33 warrant in circumstances where consent to that access is required:
34 (a) in a foreign country; or
35 (b) on a vessel or aircraft that is registered under the law of a
36 foreign country;

1 the chief officer of the law enforcement agency to which the law
2 enforcement officer who applied for the warrant belongs or is
3 seconded must give the Minister evidence in writing that the access
4 has been agreed to by an appropriate consenting official of the
5 foreign country.

6 (8) An instrument providing evidence of the kind referred to in
7 subsection (7) is not a legislative instrument.

8 (9) If a vessel or aircraft that is registered under the laws of a foreign
9 country is in or above the territorial sea of another foreign country,
10 subsections (1), (2) and (3) have effect as if the reference to an
11 appropriate consenting official of the foreign country were a
12 reference to an appropriate consenting official of each foreign
13 country concerned.

14 (10) For the avoidance of doubt, there is no requirement for the
15 agreement of an appropriate consenting official of the foreign
16 country to the access to data held in a computer under the authority
17 of a computer access warrant of a vessel or aircraft of a foreign
18 country that is in Australia or in or above waters within the outer
19 limits of the territorial sea of Australia.

20 **43B Evidence obtained from extraterritorial computer access not to**
21 **be tendered in evidence unless court satisfied properly**
22 **obtained**

23 Evidence obtained from access to data held in a computer
24 undertaken in a foreign country in accordance with
25 subsection 43A(1), (2) or (3) in relation to a relevant offence
26 cannot be tendered in evidence to a court in any proceedings
27 relating to the relevant offence unless the court is satisfied that the
28 access was agreed to by an appropriate consenting official of the
29 foreign country.

30 **88 Subsection 44(1) (after paragraph (a) of the definition of**
31 **protected information)**

32 Insert:

- 33 (aa) any information (other than general computer access
34 intercept information) obtained from access to data under:
35 (i) a computer access warrant; or
-

1 (ii) an emergency authorisation for access to data held in a
2 computer; or

3 **90 Subsection 44(1) (at the end of subparagraph (d)(iii) of the**
4 **definition of *protected information*)**

5 Add “or”.

6 **91 Subsection 44(1) (after subparagraph (d)(iii) of the**
7 **definition of *protected information*)**

8 Insert:

9 (iv) in a case where the information was obtained through
10 access to data held in a computer in a foreign country,
11 or on a vessel or aircraft that is registered under the law
12 of a foreign country and that is in or above waters
13 beyond the outer limit of Australia’s territorial sea—
14 without the agreement of the appropriate consenting
15 official of that foreign country, and of any other foreign
16 country, whose agreement is required under
17 section 43A;

18 **91A Subsection 44(1) (at the end of the definition of**
19 ***protected information*)**

20 Add:

21 Note: For protection of general computer access intercept information, see
22 Part 2-6 of the *Telecommunications (Interception and Access) Act*
23 *1979*.

24 **92 Section 46 (heading)**

25 Repeal the heading, substitute:

26 **46 Dealing with records obtained by using a surveillance device or**
27 **accessing data held in a computer**

28 **93 Paragraph 46(1)(a)**

29 After “protected information”, insert “or general computer access
30 intercept information”.

1 **94 Subsection 46(2)**

2 Omit “The officer in charge of any agency that is not a law enforcement
3 agency but that, as described in subsection 45(4) or (5) or 45A(1),
4 receives records or reports obtained by use of a surveillance device.”,
5 substitute:

6 If an agency is not a law enforcement agency but, as described in
7 subsection 45(4) or (5) or 45A(1), receives records or reports
8 obtained by:

- 9 (aa) using a surveillance device; or
10 (ab) accessing data held in a computer;
11 the officer in charge of the agency:

12 **95 After subsection 46A(1)**

13 Insert:

14 (1A) If:

- 15 (a) a record or report is in the possession of a law enforcement
16 agency; and
17 (b) the record or report comprises information obtained from
18 access to data under a control order access warrant issued on
19 the basis of a control order made in relation to a person; and
20 (c) the warrant was issued for the purpose, or for purposes that
21 include the purpose, of obtaining information that would be
22 likely to substantially assist in connection with determining
23 whether the control order, or any succeeding control order,
24 has been, or is being, complied with; and
25 (d) access to the data occurred when the control order had been
26 made, but had not come into force because it had not been
27 served on the person; and
28 (e) the chief officer of the agency is satisfied that none of the
29 information obtained from accessing the data is likely to
30 assist in connection with:
31 (i) the protection of the public from a terrorist act; or
32 (ii) preventing the provision of support for, or the
33 facilitation of, a terrorist act; or
34 (iii) preventing the provision of support for, or the
35 facilitation of, the engagement in a hostile activity in a
36 foreign country;
-

1 the chief officer of the agency must cause the record or report to be
2 destroyed as soon as practicable.

3 **96 Subsection 46A(2)**

4 After “subsection (1)”, insert “or (1A)”.

5 **97 After section 47**

6 Insert:

7 **47A Protection of computer access technologies and methods**

- 8 (1) In a proceeding, a person may object to the disclosure of
9 information on the ground that the information, if disclosed, could
10 reasonably be expected to reveal details of computer access
11 technologies or methods.
- 12 (2) If the person conducting or presiding over the proceeding is
13 satisfied that the ground of objection is made out, the person may
14 order that the person who has the information not be required to
15 disclose it in the proceeding.
- 16 (3) In determining whether or not to make an order under
17 subsection (2), the person conducting or presiding over the
18 proceeding must take into account whether disclosure of the
19 information:
20 (a) is necessary for the fair trial of the defendant; or
21 (b) is in the public interest.
- 22 (4) Subsection (2) does not affect a provision of another law under
23 which a law enforcement officer cannot be compelled to disclose
24 information or make statements in relation to the information.
- 25 (5) If the person conducting or presiding over a proceeding is satisfied
26 that publication of any information disclosed in the proceeding
27 could reasonably be expected to reveal details of computer access
28 technologies or methods, the person must make any orders
29 prohibiting or restricting publication of the information that the
30 person considers necessary to ensure that those details are not
31 revealed.

1 (6) Subsection (5) does not apply to the extent that the person
2 conducting or presiding over the proceeding considers that the
3 interests of justice require otherwise.

4 (7) In this section:

5 ***computer access technologies or methods*** means:

6 (a) technologies or methods relating to the use of:

7 (i) a computer; or

8 (ii) a telecommunications facility operated or provided by
9 the Commonwealth or a carrier; or

10 (iii) any other electronic equipment; or

11 (iv) a data storage device;

12 for the purpose of obtaining access to data held in the
13 computer; or

14 (b) technologies or methods relating to adding, copying, deleting
15 or altering other data in a computer, if doing so is necessary
16 to achieve the purpose mentioned in paragraph (a);

17 where the technologies or methods have been, or are being,
18 deployed in giving effect to:

19 (c) a computer access warrant; or

20 (d) an emergency authorisation given in response to an
21 application under subsection 28(1A), 29(1A) or 30(1A).

22 ***proceeding*** includes a proceeding before a court, tribunal or Royal
23 Commission.

24 **98 Subsection 49(2)**

25 Omit “an authorisation referred to in paragraph (1)(b) or (c),” substitute
26 “an emergency authorisation for the use of a surveillance device, or a
27 tracking device authorisation.”

28 **99 After subsection 49(2A)**

29 Insert:

30 (2B) In the case of a computer access warrant, or an emergency
31 authorisation, for access to data held in a computer, the report
32 must:

33 (a) state whether the warrant or authorisation was executed; and

- 1 (b) if so:
- 2 (i) state the name of the person primarily responsible for
- 3 the execution of the warrant or authorisation; and
- 4 (ii) state the name of each person involved in accessing data
- 5 under the warrant or authorisation; and
- 6 (iii) state the period during which the data was accessed; and
- 7 (iv) state the name, if known, of any person whose data was
- 8 accessed; and
- 9 (v) give details of any premises at which the computer was
- 10 located; and
- 11 (vi) if the warrant is issued, or the authorisation is given, in
- 12 respect of the investigation of a relevant offence—give
- 13 details of the benefit to the investigation of the accessed
- 14 data and of the general use made, or to be made, of any
- 15 evidence or information obtained by the access to data;
- 16 and
- 17 (vii) if the warrant is issued, or the authorisation is given, in
- 18 respect of the location and safe recovery of a child to
- 19 whom a recovery order relates—give details of the use
- 20 of the accessed data in assisting with the location and
- 21 safe recovery of the child; and
- 22 (viii) if the warrant is issued, or the authorisation is given, for
- 23 the purposes of an integrity operation—give details of
- 24 the benefit to the operation of the accessed data and of
- 25 the general use made, or to be made, of any evidence or
- 26 information obtained by the access to data; and
- 27 (ix) if the warrant is a control order access warrant—give
- 28 the details specified in subsection (2C); and
- 29 (x) give details of the communication of evidence or
- 30 information obtained by access to data held in the
- 31 computer to persons other than officers of the agency;
- 32 and
- 33 (xi) give details of the compliance with the conditions (if
- 34 any) to which the warrant or authorisation was subject;
- 35 and
- 36 (c) if the warrant or authorisation was extended or varied, state:
- 37 (i) the number of extensions or variations; and
- 38 (ii) the reasons for them.
-

- 1 (2C) For the purposes of subparagraph (2B)(b)(ix), the details are:
2 (a) the benefit of obtaining access to data held in the computer
3 in:
4 (i) protecting the public from a terrorist act; or
5 (ii) preventing the provision of support for, or the
6 facilitation of, a terrorist act; or
7 (iii) preventing the provision of support for, or the
8 facilitation of, the engagement in a hostile activity in a
9 foreign country; or
10 (iv) determining whether a control order has been, or is
11 being, complied with; and
12 (b) the general use to be made of any evidence or information
13 obtained by access to data held in the computer.

14 **100 Subsection 49A(1)**

15 After “control order warrant”, insert “or control order access warrant”.

16 **101 Paragraph 49A(2)(a)**

17 After “control order warrant”, insert “or control order access warrant”.

18 **102 After paragraph 49A(2)(b)**

19 Insert:

- 20 (ba) subsection 27G(2), to the extent it applies to a control order
21 access warrant;

22 **103 After paragraph 49A(2)(c)**

23 Insert:

- 24 (ca) section 45 or subsection 46(1), to the extent it applies to
25 protected information obtained, under a control order access
26 warrant, from access to data held in a computer;

27 **104 Subsection 49A(3)**

28 After “control order warrant”, insert “or control order access warrant”.

29 **105 Paragraphs 50(1)(g), (h) and (i)**

30 Repeal the paragraphs, substitute:

- 1 (g) the number of arrests made by law enforcement officers of
2 the agency during that year on the basis (wholly or partly) of
3 information obtained by:
4 (i) the use of a surveillance device under a warrant; or
5 (ii) access under a warrant to data held in a computer; or
6 (iii) an emergency authorisation for the use of a surveillance
7 device; or
8 (iv) an emergency authorisation for access to data held in a
9 computer; or
10 (v) a tracking device authorisation; and
11 (h) the number of instances during that year in which the
12 location and safe recovery of children to whom recovery
13 orders related was assisted (wholly or partly) by information
14 obtained by:
15 (i) the use of a surveillance device under a warrant; or
16 (ii) access under a warrant to data held in a computer; or
17 (iii) an emergency authorisation for the use of a surveillance
18 device; or
19 (iv) an emergency authorisation for access to data held in a
20 computer; or
21 (v) a tracking device authorisation; and
22 (i) the number of prosecutions for relevant offences that were
23 commenced during that year in which information obtained
24 by:
25 (i) the use of a surveillance device under a warrant; or
26 (ii) access under a warrant to data held in a computer; or
27 (iii) an emergency authorisation for the use of a surveillance
28 device; or
29 (iv) an emergency authorisation for access to data held in a
30 computer; or
31 (v) a tracking device authorisation;
32 was given in evidence and the number of those prosecutions
33 in which a person was found guilty; and

34 **106 Paragraph 50(1)(j)**

35 After “surveillance devices”, insert “, access to data held in computers”.

1 **107 Subsection 50A(6) (definition of *control order***
2 ***information*)**

3 Repeal the definition, substitute:

4 ***control order information*** means:

- 5 (a) information that, if made public, could reasonably be
6 expected to enable a reasonable person to conclude that a
7 control order warrant authorising:
8 (i) the use of a surveillance device on particular premises;
9 or
10 (ii) the use of a surveillance device in or on a particular
11 object or class of object; or
12 (iii) the use of a surveillance device in respect of the
13 conversations, activities or location of a particular
14 person;
15 is likely to be, or is not likely to be, in force; or
16 (b) information that, if made public, could reasonably be
17 expected to enable a reasonable person to conclude that a
18 control order access warrant authorising:
19 (i) access to data held in a particular computer; or
20 (ii) access to data held in a computer on particular premises;
21 or
22 (iii) access to data held in a computer associated with, used
23 by or likely to be used by, a particular person;
24 is likely to be, or is not likely to be, in force.

25 **108 Paragraph 51(b)**

26 Omit “or 27(4)”, substitute “, 27(4) or 27G(4)”.

27 **109 Paragraphs 52(1)(e), (f), (g) and (h)**

28 Repeal the paragraphs, substitute:

- 29 (e) details of each use by the agency, or by a law enforcement
30 officer of the agency, of information obtained by:
31 (i) the use of a surveillance device by a law enforcement
32 officer of the agency; or
33 (ii) access, by a law enforcement officer of the agency, to
34 data held in a computer;

- 1 (f) details of each communication by a law enforcement officer
2 of the agency to a person other than a law enforcement
3 officer of the agency of information obtained by:
4 (i) the use of a surveillance device by a law enforcement
5 officer of the agency; or
6 (ii) access, by a law enforcement officer of the agency, to
7 data held in a computer;
- 8 (g) details of each occasion when, to the knowledge of a law
9 enforcement officer of the agency, information obtained by:
10 (i) the use of a surveillance device by a law enforcement
11 officer of the agency; or
12 (ii) access, by a law enforcement officer of the agency, to
13 data held in a computer;
14 was given in evidence in a relevant proceeding;
- 15 (h) details of each occasion when, to the knowledge of a law
16 enforcement officer of the agency, information obtained by:
17 (i) the use of a surveillance device by a law enforcement
18 officer of the agency; or
19 (ii) access, by a law enforcement officer of the agency, to
20 data held in a computer;
21 was used in the location and safe recovery of a child to whom
22 a recovery order related;

23 **110 Paragraph 52(1)(j)**

24 After “subsection 46A(1)”, insert “or (1A)”.

25 **111 After subparagraph 53(2)(c)(iiic)**

26 Insert:

- 27 (iiid) if the warrant is a control order access warrant that was
28 issued on the basis of a control order—the date the
29 control order was made; and

30 **112 At the end of subsection 62(1)**

31 Add:

- 32 ; or (c) anything done by the law enforcement officer in connection
33 with:
34 (i) the communication by a person to another person; or

- 1 (ii) the making use of; or
2 (iii) the making of a record of; or
3 (iv) the custody of a record of;
4 information obtained from access to data under:
5 (v) a computer access warrant; or
6 (vi) an emergency authorisation for access to data held in a
7 computer.

8 **113 Subsection 62(3)**

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

10 **114 After section 64**

11 Insert:

12 **64A Person with knowledge of a computer or a computer system to**
13 **assist access etc.**

- 14 (1) A law enforcement officer (or another person on the officer’s
15 behalf) may apply to an eligible Judge or to a nominated AAT
16 member for an order (the *assistance order*) requiring a specified
17 person to provide any information or assistance that is reasonable
18 and necessary to allow the law enforcement officer to do one or
19 more of the following:
- 20 (a) access data held in a computer that is the subject of:
 - 21 (i) a computer access warrant; or
 - 22 (ii) an emergency authorisation given in response to an
23 application under subsection 28(1A), 29(1A) or 30(1A);
 - 24 (b) copy data held in the computer described in paragraph (a) to
25 a data storage device;
 - 26 (c) convert into documentary form or another form intelligible to
27 a law enforcement officer:
 - 28 (i) data held in the computer described in paragraph (a); or
 - 29 (ii) data held in a data storage device to which the data was
30 copied as described in paragraph (b).

1 *Warrants and emergency authorisations relating to relevant*
2 *offences*

3 (2) In the case of a computer that is the subject of:

- 4 (a) a computer access warrant issued in relation to a relevant
5 offence; or
6 (b) an emergency authorisation given in response to an
7 application under subsection 28(1A);

8 the eligible Judge or nominated AAT member may grant the
9 assistance order if the eligible Judge or nominated AAT member is
10 satisfied that:

11 (c) there are reasonable grounds for suspecting that access to
12 data held in the computer is necessary in the course of the
13 investigation for the purpose of enabling evidence to be
14 obtained of:

- 15 (i) the commission of those offences; or
16 (ii) the identity or location of the offenders; and

17 (d) the specified person is:

- 18 (i) reasonably suspected of having committed any of the
19 offences to which the warrant or emergency
20 authorisation relates; or
21 (ii) the owner or lessee of the computer or device; or
22 (iii) an employee of the owner or lessee of the computer or
23 device; or
24 (iv) a person engaged under a contract for services by the
25 owner or lessee of the computer or device; or
26 (v) a person who uses or has used the computer or device;
27 or
28 (vi) a person who is or was a system administrator for the
29 system including the computer or device; and

30 (e) the specified person has relevant knowledge of:

- 31 (i) the computer or device or a computer network of which
32 the computer or device forms or formed a part; or
33 (ii) measures applied to protect data held in the computer or
34 device.

- 1 *Warrants and emergency authorisations relating to recovery*
2 *orders*
- 3 (3) In the case of a computer that is the subject of:
4 (a) a computer access warrant issued in relation to a recovery
5 order; or
6 (b) an emergency authorisation given in response to an
7 application under subsection 29(1A);
8 the eligible Judge or nominated AAT member may grant the
9 assistance order if the eligible Judge or nominated AAT member is
10 satisfied that:
11 (c) there are reasonable grounds for suspecting that access to
12 data held in the computer may assist in the location and safe
13 recovery of the child to whom the recovery order relates; and
14 (d) the specified person is:
15 (i) the owner or lessee of the computer or
16 (ii) an employee of the owner or lessee of the computer; or
17 (iii) a person engaged under a contract for services by the
18 owner or lessee of the computer; or
19 (iv) a person who uses or has used the computer; or
20 (v) a person who is or was a system administrator for the
21 system including the computer; and
22 (e) the specified person has relevant knowledge of:
23 (i) the computer or a computer network of which the
24 computer forms or formed a part; or
25 (ii) measures applied to protect data held in the computer.

26 *Warrants relating to mutual assistance authorisations*

- 27 (4) In the case of a computer that is the subject of a computer access
28 warrant issued in relation to a mutual assistance authorisation, the
29 eligible Judge or nominated AAT member may grant the assistance
30 order if the eligible Judge or nominated AAT member is satisfied
31 that:
32 (a) there are reasonable grounds for suspecting that access to
33 data held in the computer is necessary, in the course of the
34 investigation or investigative proceeding to which the
35 authorisation relates, for the purpose of enabling evidence to
36 be obtained of:

- 1 (i) the commission of the offence to which the
2 authorisation relates; or
3 (ii) the identity or location of the persons suspected of
4 committing the offence; and
5 (b) the specified person is:
6 (i) reasonably suspected of committing the offence to
7 which the authorisation relates; or
8 (ii) the owner or lessee of the computer; or
9 (iii) an employee of the owner or lessee of the computer; or
10 (iv) a person engaged under a contract for services by the
11 owner or lessee of the computer; or
12 (v) a person who uses or has used the computer; or
13 (vi) a person who is or was a system administrator for the
14 system including the computer; and
15 (c) the specified person has relevant knowledge of:
16 (i) the computer or a computer network of which the
17 computer forms or formed a part; or
18 (ii) measures applied to protect data held in the computer.

19 *Warrants relating to integrity operations*

- 20 (5) In the case of a computer that is the subject of a computer access
21 warrant issued in relation to an integrity operation, the eligible
22 Judge or nominated AAT member may grant the assistance order if
23 the eligible Judge or nominated AAT member is satisfied that:
24 (a) there are reasonable grounds for suspecting that access to
25 data held in the computer will assist the conduct of the
26 integrity operation by enabling evidence to be obtained
27 relating to the integrity, location or identity of a particular
28 staff member of the target agency; and
29 (b) the specified person is:
30 (i) the staff member; or
31 (ii) the owner or lessee of the computer; or
32 (iii) an employee of the owner or lessee of the computer; or
33 (iv) a person engaged under a contract for services by the
34 owner or lessee of the computer; or
35 (v) a person who uses or has used the computer; or

- 1 (vi) a person who is or was a system administrator for the
2 system including the computer; and
3 (c) the specified person has relevant knowledge of:
4 (i) the computer or a computer network of which the
5 computer forms or formed a part; or
6 (ii) measures applied to protect data held in the computer.

7 *Warrants relating to control orders*

- 8 (6) In the case of a computer that is subject to a computer access
9 warrant issued on the basis of a control order, the eligible Judge or
10 nominated AAT member may grant the assistance order if the
11 eligible Judge or nominated AAT member is satisfied that:
12 (a) there are reasonable grounds for suspecting that access to the
13 data held in the computer would be likely to substantially
14 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 (b) the specified person is:
25 (i) the subject of the control order; or
26 (ii) the owner or lessee of the computer; or
27 (iii) an employee of the owner or lessee of the computer; or
28 (iv) a person engaged under a contract for services by the
29 owner or lessee of the computer; or
30 (v) a person who uses or has used the computer; or
31 (vi) a person who is or was a system administrator for the
32 system including the computer; and
33 (c) 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 *Emergency authorisations relating to risk of loss of evidence*

- 2 (7) In the case of a computer that is the subject of an emergency
3 authorisation given in response to an application under
4 subsection 30(1A), the eligible Judge or nominated AAT member
5 may grant the assistance order if the eligible Judge or nominated
6 AAT member is satisfied that:
- 7 (a) there are reasonable grounds for suspecting that access to
8 data held in the computer is necessary to prevent the loss of
9 any evidence relevant to the investigation to which the
10 subsection 30(1A) application relates; and
 - 11 (b) the specified person is:
 - 12 (i) reasonably suspected of having committed any of the
13 offences to which the emergency authorisation relates;
14 or
 - 15 (ii) the owner or lessee of the computer or device; or
 - 16 (iii) an employee of the owner or lessee of the computer or
17 device; or
 - 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 (c) the specified person has relevant knowledge of:
 - 25 (i) the computer or device or a computer network of which
26 the computer or device forms or formed a part; or
 - 27 (ii) measures applied to protect data held in the computer or
28 device.

29 *Offence*

- 30 (8) A person commits an offence if:
- 31 (a) the person is subject to an order under this section; and
 - 32 (b) the person is capable of complying with a requirement in the
33 order; and
 - 34 (c) the person omits to do an act; and
 - 35 (d) the omission contravenes the requirement.

1 Penalty for contravention of this subsection: Imprisonment for 10
2 years or 600 penalty units, or both.

3 **115 After subsection 65(1)**

4 Insert:

5 (1A) If:

- 6 (a) information or a record is purportedly obtained through
7 accessing, under a computer access warrant or emergency
8 authorisation, particular data held in a computer; and
9 (b) there is a defect or irregularity in relation to the warrant or
10 emergency authorisation; and
11 (c) but for that defect or irregularity, the warrant or emergency
12 authorisation would be a sufficient authority for accessing the
13 data;

14 then:

- 15 (d) access to the data is taken to be as valid; and
16 (e) the information or record obtained through accessing the data
17 may be dealt with, or given in evidence in any proceeding;
18 as if the warrant or emergency authorisation did not have that
19 defect or irregularity.

20 **116 Subsection 65(2)**

21 After “subsection (1)”, insert “or (1A)”.

22 **117 After subsection 65A(2)**

23 Insert:

24 *Control order access warrant*

25 (2A) If:

- 26 (a) a control order access warrant was issued on the basis that an
27 interim control order was in force; and
28 (b) a court subsequently declares the interim control order to be
29 void;

30 a criminal proceeding does not lie against a person in respect of
31 anything done, or omitted to be done, in good faith by the person:

- 32 (c) in the purported execution of the warrant; or
-

1 (d) in the purported exercise of a power, or the purported
2 performance of a function or duty, in a case where the
3 purported exercise of the power, or the purported
4 performance of the function or duty, is consequential on the
5 warrant.

6 (2B) Subsection (2A) does not apply to a thing done, or omitted to be
7 done, at a particular time if, at that time, the person knew, or ought
8 reasonably to have known, of the declaration.

9 **118 Section 65B (heading)**

10 Repeal the heading, substitute:

11 **65B Dealing with information obtained under a control order**
12 **warrant, control order access warrant, tracking device**
13 **authorisation etc.—control order declared to be void**

14 **119 After subparagraph 65B(1)(a)(i)**

15 Insert:

16 (ia) a control order access warrant was issued on the basis
17 that an interim control order was in force;

18 ***Telecommunications Act 1997***

19 **119A After paragraph 313(7)(c)**

20 Insert:

21 (caa) giving effect to authorisations under section 31A of that Act;
22 or

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

24 **120 Subsection 5(1)**

25 Insert:

26 ***ASIO computer access intercept information*** means information
27 obtained under:

28 (a) an ASIO computer access warrant; or

- 1 (b) subsection 25A(8) of the *Australian Security Intelligence*
2 *Organisation Act 1979*; or
3 (c) subsection 27A(3C) of the *Australian Security Intelligence*
4 *Organisation Act 1979*; or
5 (d) an authorisation under section 27E of the *Australian Security*
6 *Intelligence Organisation Act 1979*; or
7 (e) subsection 27E(6) of the *Australian Security Intelligence*
8 *Organisation Act 1979*;
9 by intercepting a communication passing over a
10 telecommunications system.

11 ***ASIO computer access warrant*** means:

- 12 (a) a warrant issued under section 25A of the *Australian Security*
13 *Intelligence Organisation Act 1979*; or
14 (b) a warrant issued under section 27A of the *Australian Security*
15 *Intelligence Organisation Act 1979* that authorises the
16 Organisation to do any of the acts or things referred to in
17 subsection 25A(4) or (8) of that Act; or
18 (c) an authorisation under section 27E of the *Australian Security*
19 *Intelligence Organisation Act 1979*.

20 ***general computer access intercept information*** means information
21 obtained under a general computer access warrant by intercepting a
22 communication passing over a telecommunications system.

23 ***general computer access warrant*** means a warrant issued under
24 section 27C of the *Surveillance Devices Act 2004*.

25 **121 Subsection 5(1) (at the end of the definition of *restricted***
26 ***record*)**

27 Add “, but does not include a record of general computer access
28 intercept information”.

29 **122 Subsection 5(1) (paragraph (b) of the definition of**
30 ***warrant*)**

31 After “definition)”, insert “, a general computer access warrant or an
32 ASIO computer access warrant”.

1 **123 After paragraph 7(2)(b)**

2 Insert:

- 3 (ba) the interception of a communication under subsection 25A(4)
4 or (8), 27A(1) or (3C), 27E(2) or 27E(6) of the *Australian*
5 *Security Intelligence Organisation Act 1979*; or
6 (bb) the interception of a communication under subsection 27E(7)
7 of the *Surveillance Devices Act 2004*; or

8 **123A Subsection 31(1)**

9 Omit “system by employees of the authority authorised under
10 section 31B.”, substitute:

11 system:

- 12 (a) if one or more carriers are specified in the request for the
13 purposes of this paragraph—by:
14 (i) employees of the security authority authorised under
15 section 31B; and
16 (ii) employees of those carriers; or
17 (b) if no carriers are specified in the request for the purposes of
18 paragraph (a)—by employees of the security authority
19 authorised under section 31B.

20 **123B Subsection 31A(1)**

21 Omit “system by employees of the security authority authorised under
22 section 31B.”, substitute:

23 system:

- 24 (a) if one or more carriers are specified in the request for the
25 purposes of paragraph 31(1)(a)—by:
26 (i) employees of the security authority authorised under
27 section 31B; and
28 (ii) employees of those carriers; or
29 (b) if no carriers are specified in the request for the purposes of
30 paragraph 31(1)(a)—by employees of the security authority
31 authorised under section 31B.

32 **123BA After subsection 31A(4)**

33 Insert:

- 1 (4A) If paragraph (1)(a) applies to the authorisation, this Part does not
2 require that an authorised interception must involve:
3 (a) one or more employees of the security authority referred to in
4 that paragraph; and
5 (b) one or more employees of a carrier referred to in that
6 paragraph;
7 acting together or in the presence of each other.

8 **123C After section 31A**

9 Insert:

10 **31AA Carrier to be notified of authorisation etc.**

- 11 (1) If:
12 (a) the Attorney-General gives a section 31A authorisation in
13 response to an application made by:
14 (i) the head (however described) of a security authority; or
15 (ii) a person acting as that head; and
16 (b) the authorisation covers the employees of a carrier;
17 the head (however described) of the security authority, or a person
18 acting as that head, must cause a copy of the authorisation to be
19 given to the authorised representative of the carrier as soon as
20 practicable.
- 21 (2) If:
22 (a) the Attorney-General has given a section 31A authorisation
23 in response to an application made by:
24 (i) the head (however described) of a security authority; or
25 (ii) a person acting as that head; and
26 (b) the authorisation is varied or revoked; and
27 (c) 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:
30 (d) an authorised representative of the carrier to be immediately
31 informed of the variation or revocation; and
32 (e) a copy of the variation or revocation to be given to the
33 authorised representative as soon as practicable.

1 **123D At the end of Part 2-4**

2 Add:

3 **31E Employees of security authorities**

4 (1) For the purposes of this Part:

5 (a) an ASIO employee is taken to be an employee of the
6 Organisation; and

7 (b) an ASIO affiliate is taken to be an employee of the
8 Organisation.

9 (2) For the purposes of this Part, if:

10 (a) a person is a staff member (within the meaning of the
11 *Intelligence Services Act 2001*) of an agency (within the
12 meaning of that Act); and

13 (b) the agency is a security authority;
14 the person is taken to be an employee of the security authority.

15 **124 After section 63AA**

16 Insert:

17 **63AB Dealing in general computer access intercept information**

18 (1) A person may, for the purposes of doing a thing authorised by a
19 general computer access warrant:

20 (a) communicate general computer access intercept information
21 to another person; or

22 (b) make use of general computer access intercept information;
23 or

24 (c) make a record of general computer access intercept
25 information; or

26 (d) give general computer access intercept information in
27 evidence in a proceeding.

28 (2) A person may:

29 (a) communicate general computer access intercept information
30 to another person; or

31 (b) make use of general computer access intercept information;
32 or

- 1 (c) make a record of general computer access intercept
2 information;
3 if the information relates, or appears to relate, to the involvement,
4 or likely involvement, of a person in one or more of the following
5 activities:
6 (d) activities that present a significant risk to a person's safety;
7 (e) acting for, or on behalf of, a foreign power (within the
8 meaning of the *Australian Security Intelligence Organisation*
9 *Act 1979*);
10 (f) activities that are, or are likely to be, a threat to security;
11 (g) activities that pose a risk, or are likely to pose a risk, to the
12 operational security (within the meaning of the *Intelligence*
13 *Services Act 2001*) of the Organisation or of ASIS, AGO or
14 ASD (within the meanings of that Act);
15 (h) activities related to the proliferation of weapons of mass
16 destruction or the movement of goods listed from time to
17 time in the Defence and Strategic Goods List (within the
18 meaning of regulation 13E of the *Customs (Prohibited*
19 *Exports) Regulations 1958*);
20 (i) activities related to a contravention, or an alleged
21 contravention, by a person of a UN sanction enforcement law
22 (within the meaning of the *Charter of the United Nations Act*
23 *1945*).

24 **63AC Dealing in ASIO computer access intercept information**

- 25 (1) A person may, for the purposes of doing a thing authorised by an
26 ASIO computer access warrant:
27 (a) communicate ASIO computer access intercept information to
28 another person; or
29 (b) make use of ASIO computer access intercept information; or
30 (c) make a record of ASIO computer access intercept
31 information; or
32 (d) give ASIO computer access intercept information in evidence
33 in a proceeding.
- 34 (2) A person may:
35 (a) communicate ASIO computer access intercept information to
36 another person; or

- 1 (b) make use of ASIO computer access intercept information; or
2 (c) make a record of ASIO computer access intercept
3 information;
4 if the information relates, or appears to relate, to the involvement,
5 or likely involvement, of a person in one or more of the following
6 activities:
7 (d) activities that present a significant risk to a person's safety;
8 (e) acting for, or on behalf of, a foreign power (within the
9 meaning of the *Australian Security Intelligence Organisation*
10 *Act 1979*);
11 (f) activities that are, or are likely to be, a threat to security;
12 (g) activities that pose a risk, or are likely to pose a risk, to the
13 operational security (within the meaning of the *Intelligence*
14 *Services Act 2001*) of the Organisation or of ASIS, AGO or
15 ASD (within the meanings of that Act);
16 (h) activities related to the proliferation of weapons of mass
17 destruction or the movement of goods listed from time to
18 time in the Defence and Strategic Goods List (within the
19 meaning of regulation 13E of the *Customs (Prohibited*
20 *Exports) Regulations 1958*);
21 (i) activities related to a contravention, or an alleged
22 contravention, by a person of a UN sanction enforcement law
23 (within the meaning of the *Charter of the United Nations Act*
24 *1945*).

25 **124A At the end of section 63B**

26 Add:

- 27 (5) If an employee of a carrier has obtained lawfully intercepted
28 information under a section 31A authorisation that was given in
29 response to an application made by the head (however described)
30 of a security authority or a person acting as that head, the employee
31 may:
32 (a) communicate the information to:
33 (i) an employee of the security authority; or
34 (ii) another employee of the carrier; or
35 (iii) if the authorisation covers the employees of one or more
36 other carriers—an employee of any of those other
37 carriers; or

- 1 (b) make use of the information; or
2 (c) make a record of the information;
3 if:
4 (d) the employee does so for the purposes of the development or
5 testing of technologies, or interception capabilities, to which
6 the authorisation relates; and
7 (e) the communication or use of the information, or the making
8 of the record, as the case may be, does not contravene a
9 condition to which the authorisation is subject.

10 **125 Paragraph 64(1)(a)**

11 After “foreign intelligence information”, insert “or ASIO computer
12 access intercept information”.

13 **126 Paragraph 65(1)(a)**

14 After “information”, insert “other than ASIO computer access intercept
15 information”.

16 **126AA At the end of section 65 (after the note)**

17 Add:

- 18 (4) If lawfully intercepted information was obtained under a
19 section 31A authorisation, subsection (1) of this section does not
20 authorise the communication of the information in accordance with
21 subsection 18(3) of the *Australian Security Intelligence*
22 *Organisation Act 1979* to:
23 (a) a staff member of an authority of the Commonwealth; or
24 (b) a staff member of an authority of a State;
25 unless the communication is for the purpose of the development or
26 testing of technologies, or interception capabilities, of:
27 (c) that authority; or
28 (d) the Organisation.
- 29 (5) If lawfully intercepted information was obtained under a
30 section 31A authorisation, subsection (1) of this section does not
31 authorise the communication of the information in accordance with
32 subsection 18(4A) of the *Australian Security Intelligence*
33 *Organisation Act 1979* to a staff member of ASIS, ASD or AGO

- 1 unless the communication is for the purpose of the development or
2 testing of technologies, or interception capabilities, of:
3 (a) ASIS, ASD or AGO, as the case requires; or
4 (b) the Organisation.
- 5 (6) If lawfully intercepted information was obtained under a
6 section 31A authorisation, subsection (1) of this section does not
7 authorise the communication of the information in accordance with
8 subsection 19A(4) of the *Australian Security Intelligence*
9 *Organisation Act 1979* to a staff member of a body referred to in
10 paragraph 19A(1)(d) or (e) of that Act unless the communication is
11 for the purpose of the development or testing of technologies, or
12 interception capabilities, of:
13 (a) that body; or
14 (b) the Organisation.
- 15 (7) For the purposes of subsections (4), (5) and (6), *authority of the*
16 *Commonwealth, authority of a State, ASIS, ASD, AGO* and *staff*
17 *member* have the same respective meanings as in the *Australian*
18 *Security Intelligence Organisation Act 1979*.

19 **126A Paragraph 65A(1)(a)**

20 After “foreign intelligence information”, insert “or information obtained
21 under a section 31A authorisation”.

22 **127 Paragraph 67(1)(a)**

23 After “foreign intelligence information”, insert “or general computer
24 access intercept information”.

25 **128 Section 68**

26 After “communicate lawfully intercepted information”, insert “(other
27 than general computer access intercept information)”.

28 **129 Subsection 74(1)**

29 After “foreign intelligence information”, insert “, general computer
30 access intercept information or ASIO computer access intercept
31 information”.

Schedule 2 Computer access warrants etc.

Part 1 Amendments

1 **130 Subsection 75(1)**

2 After “other than”, insert “a general computer access warrant or”.

3 **131 Paragraphs 77(1)(a) and (b)**

4 After “63A,”, insert “63AB, 63AC,”.

5 **131A After paragraph 108(2)(ca)**

6 Insert:

7 (cb) accessing a stored communication under a general computer
8 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

- 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

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 (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:

- 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 **11 After subsection 3ZQV(3)**

18 Insert:

- 19 (3A) If the electronic equipment was seized under a warrant,
20 subsection (2) does not apply to data that was generated after the
21 expiry of the warrant.

22 **12 Application of amendments**

23 The amendments of sections 3F, 3K, 3LAA, 3LA, 3N and 3ZQV of the
24 *Crimes Act 1914* made by this Schedule apply in relation to a warrant
25 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 **19 Subsection 203K(5)**

4 After “198(1),”, insert “199A(1),”.

5 **20 Subsection 203M(4)**

6 After “198,”, insert “199A,”.

7 **21 Application of amendments**

- 8 (1) The amendments of sections 199, 200 and 201A of the *Customs Act*
9 *1901* made by this Schedule apply in relation to a warrant issued after
10 the commencement of this item.
- 11 (2) Section 201AA of the *Customs Act 1901* (as amended by this Schedule)
12 applies in relation to a warrant issued after the commencement of this
13 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:

- 31 (a) orally; or
-

- 1 (b) in writing.
- 2 (3) If a request under paragraph (1)(a) is made orally, the
3 Director-General must:
- 4 (a) make a written record of the request; and
5 (b) do so within 48 hours after the request was made.
- 6 (4) The Director-General may enter into a contract, agreement or
7 arrangement with a person or body in relation to conduct engaged
8 in by the person or body in accordance with a request under
9 paragraph (1)(a).

10 *Unsolicited disclosure of information etc.*

- 11 (5) If:
- 12 (a) a person or body engages in conduct that consists of, or is
13 connected with:
- 14 (i) giving information to the Organisation; or
15 (ii) giving or producing a document to the Organisation; or
16 (iii) making one or more copies of a document and giving
17 those copies to the Organisation; and
- 18 (b) the person reasonably believes that the conduct is likely to
19 assist the Organisation in the performance of its functions;
20 and
- 21 (c) the conduct does not involve the person or body committing
22 an offence against a law of the Commonwealth, a State or a
23 Territory; and
- 24 (d) the conduct does not result in significant loss of, or serious
25 damage to, property; and
- 26 (e) subsection (1) does not apply to the conduct;
- 27 the person or body is not subject to any civil liability for, or in
28 relation to, the conduct.

29 *Copies of, or extracts from, documents*

- 30 (6) The Organisation may make and retain copies of, or take and retain
31 extracts from, a document given or produced to the Organisation:
- 32 (a) in accordance with a request under paragraph (1)(a); or
33 (b) under paragraph (5)(a).

1 **Subdivision J—Assistance relating to access to data**

2 **34AAA Person with knowledge of a computer or a computer system**
3 **to assist access to data**

4 (1) The Director-General may request the Attorney-General to make
5 an order requiring a specified person to provide any information or
6 assistance that is reasonable and necessary to allow the
7 Organisation to do one or more of the following:

8 (a) access data held in, or accessible from, a computer or data
9 storage device that:

10 (i) is the subject of a warrant under section 25A, 26 or
11 27A; or

12 (ii) is the subject of an authorisation under section 27E or
13 27F; or

14 (iii) is on premises in relation to which a warrant under
15 section 25, 26 or 27A is in force; or

16 (iv) is on premises in relation to which an authorisation
17 under section 27D or 27F is in force; or

18 (v) is found in the course of an ordinary search of a person,
19 or a frisk search of a person, authorised by a warrant
20 under section 25 or 27A; or

21 (vi) is found in the course of an ordinary search of a person,
22 or a frisk search of a person, authorised under
23 section 27D; or

24 (vii) has been removed from premises under a warrant under
25 section 25, 26 or 27A; or

26 (viii) has been removed from premises under section 27D; or

27 (ix) has been seized under section 34ZB;

28 (b) copy data held in, or accessible from, a computer, or data
29 storage device, described in paragraph (a) to another data
30 storage device;

31 (c) convert into documentary form or another form intelligible to
32 an ASIO employee or ASIO affiliate:

33 (i) data held in, or accessible from, a computer, or data
34 storage device, described in paragraph (a); or

35 (ii) data held in a data storage device to which the data was
36 copied as described in paragraph (b); or

-
- 1 (iii) data held in a computer or data storage device removed
 2 from premises under a warrant under section 25, 26 or
 3 27A; or
 4 (iv) data held in a computer or data storage device removed
 5 from premises under section 27D.
- 6 (2) The Attorney-General may make the order if:
- 7 (a) in a case where the computer or data storage device:
- 8 (i) is the subject of a warrant under section 27A; or
 9 (ii) is on premises in relation to which a warrant under
 10 section 27A is in force; or
 11 (iii) is found in the course of an ordinary search of a person,
 12 or a frisk search of a person, authorised by a warrant
 13 under section 27A; or
 14 (iv) has been removed from premises under a warrant under
 15 section 27A;
- 16 the Attorney-General is satisfied, on reasonable grounds,
 17 that:
- 18 (v) access by the Organisation to data held in, or accessible
 19 from, the computer or data storage device will be for the
 20 purpose of obtaining foreign intelligence relating to a
 21 matter specified in the relevant notice under
 22 subsection 27A(1); and
 23 (vi) on the basis of advice received from the Defence
 24 Minister or the Foreign Affairs Minister, the collection
 25 of foreign intelligence relating to that matter is in the
 26 interests of Australia's national security, Australia's
 27 foreign relations or Australia's national economic
 28 well-being; and
- 29 (b) in a case where paragraph (a) does not apply—the
 30 Attorney-General is satisfied that there are reasonable
 31 grounds for suspecting that access by the Organisation to data
 32 held in, or accessible from, the computer or data storage
 33 device will substantially assist the collection of intelligence
 34 in accordance with this Act in respect of a matter that is
 35 important in relation to security; and
- 36 (c) the Attorney-General is satisfied, on reasonable grounds, that
 37 the specified person is:

- 1 (i) reasonably suspected of being involved in activities that
2 are prejudicial to security; or
3 (ii) the owner or lessee of the computer or device; or
4 (iii) an employee of the owner or lessee of the computer or
5 device; or
6 (iv) a person engaged under a contract for services by the
7 owner or lessee of the computer or device; or
8 (v) a person who uses or has used the computer or device;
9 or
10 (vi) a person who is or was a system administrator for the
11 system including the computer or device; and
12 (d) the Attorney-General is satisfied, on reasonable grounds, that
13 the specified person has relevant knowledge of:
14 (i) the computer or device or a computer network of which
15 the computer or device forms or formed a part; or
16 (ii) measures applied to protect data held in, or accessible
17 from, the computer or device.
- 18 (3) If the computer or data storage device is not on premises in relation
19 to which a warrant is in force, the order must:
20 (a) specify the period within which the person must provide the
21 information or assistance; and
22 (b) specify the place at which the person must provide the
23 information or assistance; and
24 (c) specify the conditions (if any) determined by the
25 Attorney-General as the conditions to which the requirement
26 on the person to provide the information or assistance is
27 subject.
- 28 (4) A person commits an offence if:
29 (a) the person is subject to an order under this section; and
30 (b) the person is capable of complying with a requirement in the
31 order; and
32 (c) the person omits to do an act; and
33 (d) the omission contravenes the requirement.
- 34 Penalty for contravention of this subsection: Imprisonment for 5
35 years or 300 penalty units, or both.