

EXPOSURE DRAFT

2016-2017-2018

The Parliament of the
Commonwealth of Australia

HOUSE OF REPRESENTATIVES

EXPOSURE DRAFT

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**

EXPOSURE DRAFT

EXPOSURE DRAFT

Contents

1	Short title.....	1
2	Commencement.....	1
3	Schedules.....	3
Schedule 1—Industry assistance		4
	<i>Administrative Decisions (Judicial Review) Act 1977</i>	4
	<i>Criminal Code Act 1995</i>	4
	<i>Telecommunications Act 1997</i>	5
Schedule 2—Computer access warrants etc.		65
Part 1—Amendments		65
	<i>Australian Security Intelligence Organisation Act 1979</i>	65
	<i>Mutual Assistance in Criminal Matters Act 1987</i>	71
	<i>Surveillance Devices Act 2004</i>	73
	<i>Telecommunications Act 1997</i>	127
	<i>Telecommunications (Interception and Access) Act 1979</i>	127
Part 2—Application provisions		137
Part 3—Amendments contingent on the commencement of the Crimes Legislation Amendment (International Crime Cooperation and Other Measures) Act 2018		138
	<i>International Criminal Court Act 2002</i>	138
	<i>International War Crimes Tribunals Act 1995</i>	139
	<i>Surveillance Devices Act 2004</i>	140
Schedule 3—Search warrants issued under the Crimes Act 1914		144
	<i>Crimes Act 1914</i>	144
Schedule 4—Search warrants issued under the Customs Act 1901		154
	<i>Customs Act 1901</i>	154
Schedule 5—Australian Security Intelligence Organisation		166

EXPOSURE DRAFT

Australian Security Intelligence Organisation Act 1979

166

ii Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 No. , 2018

EXPOSURE DRAFT

EXPOSURE DRAFT

column 2 of the table. Any other statement in column 2 has effect according to its terms.

Commencement information

Column 1	Column 2	Column 3
Provisions	Commencement	Date/Details
1. Sections 1 to 3 and anything in this Act not elsewhere covered by this table	The day this Act receives the Royal Assent.	
2. Schedule 1	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 2, Parts 1 and 2	The day after this Act receives the Royal Assent.	
4. 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.	
5. Schedules 3, 4 and 5	The day after this Act receives the Royal Assent.	

Note: This table relates only to the provisions of this Act as originally enacted.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

EXPOSURE DRAFT

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

4 **3 Schedules**

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

EXPOSURE DRAFT

Schedule 1 Industry assistance

1 **Schedule 1—Industry assistance**
2

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

28

- 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
 - (c) protecting the public revenue; or

EXPOSURE DRAFT

Schedule 1 Industry assistance

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

- (d) 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) protecting the public revenue; or
 - (d) 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) protecting the public revenue; or
 - (d) 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

EXPOSURE DRAFT

Industry assistance **Schedule 1**

1
2
3
4
5
6
7
8
9
10
11
12
13

- (b) assisting the enforcement of the criminal laws in force in a foreign country; or
 - (c) protecting the public revenue; or
 - (d) safeguarding national security.
- 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) protecting the public revenue; or
 - (d) safeguarding national security.

14

317B Definitions

15

In this Part:

16

access, when used in relation to material, includes:

17

(a) access that is subject to a pre-condition (for example, the use of a password); and

18

19

(b) access by way of push technology; and

20

(c) access by way of a standing request.

21

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

22

23

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

24

25

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

26

27

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

28

29

30

31

EXPOSURE DRAFT

Industry assistance Schedule 1

1 (c) when used in relation to the Australian Signals Directorate—
2 includes giving help to a staff member of the Australian
3 Signals Directorate; or

4 (d) when used in relation to an interception agency—includes
5 giving help to an officer of the agency.

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

8 ***Independent Broad-based Anti-corruption Commission of***
9 ***Victoria*** means the Independent Broad-based Anti-corruption
10 Commission established by the *Independent Broad-based*
11 *Anti-corruption Commission Act 2011* (Vic).

12 ***Independent Commissioner Against Corruption (SA)*** means the
13 person who is the Commissioner (within the meaning of the
14 *Independent Commissioner Against Corruption Act 2012* (SA)).

15 ***interception agency*** means:

16 (a) the Australian Federal Police; or

17 (b) the Australian Commission for Law Enforcement Integrity;
18 or

19 (c) the Australian Crime Commission; or

20 (d) the Police Force of a State or the Northern Territory; or

21 (e) the Independent Commission Against Corruption of New
22 South Wales; or

23 (f) the New South Wales Crime Commission; or

24 (g) the Law Enforcement Conduct Commission of New South
25 Wales; or

26 (h) the Independent Broad-based Anti-corruption Commission of
27 Victoria; or

28 (i) the Crime and Corruption Commission of Queensland; or

29 (j) the Independent Commissioner Against Corruption (SA); or

30 (k) the Corruption and Crime Commission (WA).

31 ***Law Enforcement Conduct Commission of New South Wales***
32 means the Law Enforcement Conduct Commission constituted by
33 the *Law Enforcement Conduct Commission Act 2016* (NSW).

EXPOSURE DRAFT

Schedule 1 Industry assistance

- 1 *listed act or thing* has the meaning given by section 317E.
- 2 *material* means material:
- 3 (a) whether in the form of text; or
- 4 (b) whether in the form of data; or
- 5 (c) whether in the form of speech, music or other sounds; or
- 6 (d) whether in the form of visual images (moving or otherwise);
- 7 or
- 8 (e) whether in any other form; or
- 9 (f) whether in any combination of forms.
- 10 *member of the staff of the Independent Commissioner Against*
- 11 *Corruption (SA)* means a person who is engaged under
- 12 subsection 12(1) of the *Independent Commissioner Against*
- 13 *Corruption Act 2012 (SA)*.
- 14 *officer* of an interception agency has the meaning given by
- 15 section 317ZM.
- 16 *staff member*, when used in relation to the Australian Secret
- 17 Intelligence Service or the Australian Signals Directorate, has the
- 18 same meaning as in the *Intelligence Services Act 2001*.
- 19 *supply*:
- 20 (a) when used in relation to:
- 21 (i) a facility; or
- 22 (ii) customer equipment; or
- 23 (iii) a component;
- 24 includes supply (including re-supply) by way of sale,
- 25 exchange, lease, hire or hire-purchase; and
- 26 (b) when used in relation to software—includes provide, grant or
- 27 confer rights, privileges or benefits.
- 28 *technical assistance notice* means a notice given under
- 29 section 317L.
- 30 *technical assistance notice information* means:
- 31 (a) information about any of the following:
- 32 (i) the giving of a technical assistance notice;

EXPOSURE DRAFT

Industry assistance **Schedule 1**

- 1 (ii) the existence or non-existence of a technical assistance
2 notice;
- 3 (iii) the variation of a technical assistance notice;
- 4 (iv) the revocation of a technical assistance notice;
- 5 (v) the requirements imposed by a technical assistance
6 notice;
- 7 (vi) any act or thing done in compliance with a technical
8 assistance notice; or
- 9 (b) any other information about a technical assistance notice.

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

12 ***technical assistance request information*** means:

- 13 (a) information about any of the following:
 - 14 (i) the giving of a technical assistance request;
 - 15 (ii) the existence or non-existence of a technical assistance
16 request;
 - 17 (iii) the acts or things covered by a technical assistance
18 request;
 - 19 (iv) any act or thing done in accordance with a technical
20 assistance request; or
- 21 (b) any other information about a technical assistance request.

22 ***technical capability notice*** means a notice given under
23 section 317T.

24 ***technical capability notice information*** means:

- 25 (a) information about any of the following:
 - 26 (i) the giving of a technical capability notice;
 - 27 (ii) consultation relating to the giving of a technical
28 capability notice;
 - 29 (iii) the existence or non-existence of a technical capability
30 notice;
 - 31 (iv) the variation of a technical capability notice;
 - 32 (v) the revocation of a technical capability notice;
 - 33 (vi) the requirements imposed by a technical capability
34 notice;
-

EXPOSURE DRAFT

Schedule 1 Industry assistance

- 1 (vii) any act or thing done in compliance with a technical
2 capability notice; or
3 (b) any other information about a technical capability notice.

4 **317C Designated communications provider etc.**

- 5 For the purposes of this Part, the following table defines:
6 (a) *designated communications provider*; and
7 (b) the *eligible activities* of a designated communications
8 provider.
9

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	the provision by the person of a

12 *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* No. , 2018

EXPOSURE DRAFT

Industry assistance **Schedule 1**

Designated communications provider and eligible activities		
Item	A person is a designated communications provider if and the eligible activities of the person are ...
	facilitates, or is ancillary or incidental to, the provision of an electronic service that has one or more end-users in Australia	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 (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	(a) the manufacture by the person of

EXPOSURE DRAFT

Schedule 1 Industry assistance

Designated communications provider and eligible activities		
Item	A person is a designated communications provider if and the eligible activities of the person are ...
	components for use, or likely to be used, in the manufacture of customer equipment for use, or likely to be used, in Australia	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 (b) does so otherwise than in the capacity of end-user of the equipment	any such connection by the person of customer equipment to a telecommunications network in Australia
14	the person is a constitutional corporation who: (a) manufactures; or (b) supplies; or (c) installs; or (d) maintains; data processing devices	(a) the manufacture by the person of data processing devices for use, or likely to be used, in Australia; or (b) the supply by the person of data processing devices for use, or likely to be used, in Australia; or (c) the installation by the person of data processing devices in Australia; or (d) the maintenance by the person of data processing devices in Australia
15	the person is a constitutional corporation who: (a) develops; or (b) supplies; or (c) updates;	(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

14 *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* No. , 2018

EXPOSURE DRAFT

Industry assistance Schedule 1

Designated communications provider and eligible activities

Item	A person is a designated communications provider if and the eligible activities of the person are ...
------	---	---

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

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

2 **317D Electronic service**

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

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

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

7
8 but does not include:

9 (c) a broadcasting service; or

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

11
12
13 (2) For the purposes of subsection (1), *service* includes a website.

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

15
16
17 (4) For the purposes of this Part, a person does not provide an electronic service merely because the person provides a billing service, or a fee collection service, in relation to an electronic service.

18
19
20
21 (5) A reference in this section to the *use* of a thing is a reference to the use of the thing either:

22 (a) in isolation; or

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

EXPOSURE DRAFT

Schedule 1 Industry assistance

1 **317E Listed acts or things**

- 2 (1) For the purposes of the application of this Part to a designated
3 communications provider, *listed act or thing* means:
- 4 (a) removing one or more forms of electronic protection that are
5 or were applied by, or on behalf of, the provider; or
- 6 (b) providing technical information; or
- 7 (c) installing, maintaining, testing or using software or
8 equipment; or
- 9 (d) ensuring that information obtained in connection with the
10 execution of a warrant or authorisation is given in a particular
11 format; or
- 12 (e) facilitating or assisting access to whichever of the following
13 are the subject of eligible activities of the provider:
- 14 (i) a facility;
- 15 (ii) customer equipment;
- 16 (iii) a data processing device;
- 17 (iv) a listed carriage service;
- 18 (v) a service that facilitates, or is ancillary or incidental to,
19 the supply of a listed carriage service;
- 20 (vi) an electronic service;
- 21 (vii) a service that facilitates, or is ancillary or incidental to,
22 the provision of an electronic service;
- 23 (viii) software used, for use, or likely to be used, in
24 connection with a listed carriage service;
- 25 (ix) software used, for use, or likely to be used, in
26 connection with an electronic service;
- 27 (x) software that is capable of being installed on a
28 computer, or other equipment, that is, or is likely to be,
29 connected to a telecommunications network; or
- 30 (f) assisting with the testing, modification, development or
31 maintenance of a technology or capability; or
- 32 (g) notifying particular kinds of changes to, or developments
33 affecting, eligible activities of the designated
34 communications provider, if the changes are relevant to the
35 execution of a warrant or authorisation; or

- 1 (h) modifying, or facilitating the modification of, any of the
2 characteristics of a service provided by the designated
3 communications provider; or
4 (i) substituting, or facilitating the substitution of, a service
5 provided by the designated communications provider for:
6 (i) another service provided by the provider; or
7 (ii) a service provided by another designated
8 communications provider; or
9 (j) an act or thing done to conceal the fact that any thing has
10 been done covertly in the performance of a function, or the
11 exercise of a power, conferred by a law of the
12 Commonwealth, a State or a Territory, so far as the function
13 or power relates to:
14 (i) enforcing the criminal law and laws imposing pecuniary
15 penalties; or
16 (ii) assisting the enforcement of the criminal laws in force
17 in a foreign country; or
18 (iii) protecting the public revenue; or
19 (iv) the interests of Australia's national security, the
20 interests of Australia's foreign relations or the interests
21 of Australia's national economic well-being.
- 22 (2) Paragraph (1)(j) does not apply to:
23 (a) making a false or misleading statement; or
24 (b) engaging in dishonest conduct.

25 **317F Extension to external Territories**

26 This Part extends to every external Territory.

27 **Division 2—Voluntary technical assistance**

28 **317G Voluntary technical assistance provided to ASIO, the** 29 **Australian Secret Intelligence Service, the Australian** 30 **Signals Directorate or an interception agency**

- 31 (1) If:
32 (a) any of the following persons:
-

EXPOSURE DRAFT

Schedule 1 Industry assistance

- 1 (i) the Director-General of Security;
2 (ii) the Director-General of the Australian Secret
3 Intelligence Service;
4 (iii) the Director-General of the Australian Signals
5 Directorate;
6 (iv) the chief officer of an interception agency;
7 requests a designated communications provider to do one or
8 more specified acts or things that:
9 (v) are in connection with any or all of the eligible activities
10 of the provider; and
11 (vi) are covered by subsection (2); and
12 (b) the provider does an act or thing:
13 (i) in accordance with the request; or
14 (ii) in good faith purportedly in accordance with the
15 request;
16 then:
17 (c) the provider is not subject to any civil liability for, or in
18 relation to, the act or thing mentioned in paragraph (b); and
19 (d) an officer, employee or agent of the provider is not subject to
20 any civil liability for, or in relation to, an act or thing done by
21 the officer, employee or agent in connection with the act or
22 thing mentioned in paragraph (b).
- 23 (2) The specified acts or things must:
24 (a) be directed towards ensuring that the designated
25 communications provider is capable 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:
-

EXPOSURE DRAFT

Industry assistance **Schedule 1**

- 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); or
7 (b) be by way 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).
- 25 (3) A request under paragraph (1)(a) is to be known as a *technical*
26 *assistance request*.
- 27 (4) Subparagraph (1)(b)(ii) does not apply to an act or thing done by a
28 designated communications provider unless the act or thing is in
29 connection with any or all of the eligible activities of the provider.
- 30 *Relevant objective*
- 31 (5) For the purposes of this section, *relevant objective* means:
32 (a) enforcing the criminal law and laws imposing pecuniary
33 penalties; or
34 (b) assisting the enforcement of the criminal laws in force in a
35 foreign country; or
-

EXPOSURE DRAFT

EXPOSURE DRAFT

Schedule 1 Industry assistance

- 1 (c) protecting the public revenue; or
2 (d) the interests of Australia's national security, the interests of
3 Australia's foreign relations or the interests of Australia's
4 national economic well-being.

5 *Listed acts or things*

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

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

14 **317H Form of technical assistance request**

- 15 (1) A technical assistance request may be given:
16 (a) orally; or
17 (b) in writing.
- 18 (2) A technical assistance request must not be given orally unless:
19 (a) an imminent risk of serious harm to a person or substantial
20 damage to property exists; and
21 (b) the technical assistance request is necessary for the purpose
22 of dealing with that risk; and
23 (c) it is not practicable in the circumstances to give the technical
24 assistance request in writing.
- 25 (3) If a technical assistance request is given orally by:
26 (a) the Director-General of Security; or
27 (b) the Director-General of the Australian Secret Intelligence
28 Service; or
29 (c) the Director-General of the Australian Signals Directorate; or
30 (d) the chief officer of an interception agency;
31 the Director-General of Security, the Director-General of the
32 Australian Secret Intelligence Service, the Director-General of the

- 1 Australian Signals Directorate or the chief officer, as the case
2 requires, must:
- 3 (e) make a written record of the request; and
4 (f) do so within 48 hours after the request was given.
- 5 (4) If, under subsection (3):
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 makes a written record of a technical assistance request, the
12 Director-General of Security, the Director-General of the
13 Australian Secret Intelligence Service, the Director-General of the
14 Australian Signals Directorate or the chief officer, as the case
15 requires, must:
16 (e) give a copy of the record to the designated communications
17 provider concerned; and
18 (f) do so as soon as practicable after the record was made.

19 **317HA Duration of technical assistance request**

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

EXPOSURE DRAFT

Schedule 1 Industry assistance

317J Specified period etc.

- 1
- 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).

317JA Variation of technical assistance requests

- 10
- 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:

EXPOSURE DRAFT

Industry assistance **Schedule 1**

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

EXPOSURE DRAFT

Schedule 1 Industry assistance

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

11 **317JB Revocation of technical assistance requests**

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

26 **317K Contract etc.**

- 27 Any of the following persons:
28 (a) the Director-General of Security;
29 (b) the Director-General of the Australian Secret Intelligence
30 Service;
31 (c) the Director-General of the Australian Signals Directorate;

- 1 (d) the chief officer of an interception agency;
2 may enter into a contract, agreement or arrangement with a
3 designated communications provider in relation to acts or things
4 done by the provider in accordance with a technical assistance
5 request.

6 **Division 3—Technical assistance notices**

7 **317L Technical assistance notices**

- 8 (1) The Director-General of Security or the chief officer of an
9 interception agency may give a designated communications
10 provider a notice, to be known as a technical assistance notice, that
11 requires the provider to do one or more specified acts or things
12 that:

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

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

- 18 (2) The specified acts or things must be by way of giving help to:
19 (a) in a case where the technical assistance notice is given by the
20 Director-General of Security—ASIO; or
21 (b) in a case where the technical assistance notice is given by the
22 chief officer of an interception agency—the agency;
23 in relation to:
24 (c) the performance of a function, or the exercise of a power,
25 conferred by or under a law of the Commonwealth, a State or
26 a Territory, so far as the function or power relates to:
27 (i) enforcing the criminal law and laws imposing pecuniary
28 penalties; or
29 (ii) assisting the enforcement of the criminal laws in force
30 in a foreign country; or
31 (iii) protecting the public revenue; or
32 (iv) safeguarding national security; or
33 (d) a matter that facilitates, or is ancillary or incidental to, a
34 matter covered by paragraph (c).
-

EXPOSURE DRAFT

Schedule 1 Industry assistance

1

Listed acts or things

2

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

3

4

5

6

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

7

8

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

9

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

10

317M Form of technical assistance notice

11

- (1) A technical assistance notice may be given:

12

- (a) orally; or

13

- (b) in writing.

14

- (2) A technical assistance notice must not be given orally unless:

15

- (a) an imminent risk of serious harm to a person or substantial damage to property exists; and

16

17

- (b) the technical assistance notice is necessary for the purpose of dealing with that risk; and

18

19

- (c) it is not practicable in the circumstances to give the technical assistance notice in writing.

20

21

- (3) If a technical assistance notice is given orally by the

22

Director-General of Security or the chief officer of an interception agency, the Director-General of Security or the chief officer, as the case requires, must:

23

24

- (a) make a written record of the notice; and

25

26

- (b) do so within 48 hours after the notice was given.

27

- (4) If, under subsection (3), the Director-General of Security or the chief officer of an interception agency makes a written record of a technical assistance notice, the Director-General of Security or the chief officer, as the case requires, must:

28

29

30

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

31

32

33

- (b) do so as soon as practicable after the record was made.
-

26

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

No. , 2018

EXPOSURE DRAFT

1 **317MA Duration of technical assistance notice**

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

15 **317N Compliance period etc.**

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

24 **317P Decision-making criteria**

25 The Director-General of Security or the chief officer of an
26 interception agency must not give a technical assistance notice to a
27 designated communications provider unless the Director-General
28 of Security or the chief officer, as the case requires, is satisfied
29 that:

- 30 (a) the requirements imposed by the notice are reasonable and
31 proportionate; and
-

EXPOSURE DRAFT

Schedule 1 Industry assistance

- 1 (b) compliance with the notice is:
2 (i) practicable; and
3 (ii) technically feasible.

4 **317Q Variation of technical assistance notices**

- 5 (1) If a technical assistance notice has been given to a designated
6 communications provider by the Director-General of Security, the
7 Director-General of Security may vary the notice.
- 8 (2) If a technical assistance notice has been given to a designated
9 communications provider by the chief officer of an interception
10 agency, the chief officer may vary the notice.

11 *Form of variation*

- 12 (3) A variation may be made:
13 (a) orally; or
14 (b) in writing.
- 15 (4) A variation must not be made orally unless:
16 (a) an imminent risk of serious harm to a person or substantial
17 damage to property exists; and
18 (b) the variation is necessary for the purpose of dealing with that
19 risk; and
20 (c) it is not practicable in the circumstances to make the
21 variation in writing.
- 22 (5) If a variation is made orally by the Director-General of Security or
23 the chief officer of an interception agency, the Director-General of
24 Security or the chief officer, as the case requires, must:
25 (a) make a written record of the variation; and
26 (b) do so within 48 hours after the variation was made.
- 27 (6) If, under subsection (5), the Director-General of Security or the
28 chief officer of an interception agency makes a written record of a
29 variation, the Director-General of Security or the chief officer, as
30 the case requires, must:

EXPOSURE DRAFT

Industry assistance **Schedule 1**

1 (a) give a copy of the record to the designated communications
2 provider concerned; and

3 (b) do so as soon as practicable after the record was made.

4 (7) If a variation is made in writing by the Director-General of
5 Security or the chief officer of an interception agency, the
6 Director-General of Security or the chief officer, as the case
7 requires, must:

8 (a) give a copy of the variation to the designated
9 communications provider concerned;

10 (b) do so as soon as practicable after the variation was made.

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

12 (8) The acts or things specified in a varied technical assistance notice
13 must be:

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

16 (b) covered by subsection 317L(2).

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

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

22 (b) are covered by subsection 317L(2).

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

24 *Decision-making criteria*

25 (10) The Director-General of Security or the chief officer of an
26 interception agency must not vary a technical assistance notice
27 unless the Director-General of Security or the chief officer, as the
28 case requires, is satisfied that:

29 (a) the requirements imposed by the varied notice are reasonable
30 and proportionate; and

31 (b) compliance with the varied notice is:

32 (i) practicable; and

33 (ii) technically feasible.

EXPOSURE DRAFT

Schedule 1 Industry assistance

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

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

1 **Division 4—Technical capability notices**

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

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

15 **317T Technical capability notices**

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

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

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

EXPOSURE DRAFT

Schedule 1 Industry assistance

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

13 *Relevant objective*

- 14 (3) For the purposes of this section, ***relevant objective*** means:
15 (a) enforcing the criminal law and laws imposing pecuniary
16 penalties; or
17 (b) assisting the enforcement of the criminal laws in force in a
18 foreign country; or
19 (c) protecting the public revenue; or
20 (d) safeguarding national security.

21 *Listed help*

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

EXPOSURE DRAFT

Industry assistance **Schedule 1**

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

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

13 *Listed acts or things*

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

22 *Limits*

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

EXPOSURE DRAFT

Schedule 1 Industry assistance

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

4 (e) has a delivery capability.

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

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

9 (9) For the purposes of subsection (8), ensuring that a kind of service
10 or a system has a particular capability includes ensuring that the
11 capability is developed, installed and maintained.

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

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

18 (b) documents containing information of that kind;
19 relating to any communication carried by means of a service to
20 which Part 5-1A of the *Telecommunications (Interception and*
21 *Access) Act 1979* applies.

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

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

28 *Applicable costs negotiator*

29 (12) A technical capability notice must specify a person as the
30 applicable costs negotiator for the notice.

31 Note: See section 317ZK.

32 (13) A person may be specified under subsection (12):

33 (a) by name; or

- 1 (b) as any person from time to time holding, occupying, or
2 performing the duties of, a specified office or position.

3 **317TA Duration of technical capability notice**

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

17 **317U Compliance period etc.**

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

26 **317V Decision-making criteria**

- 27 The Attorney-General must not give a technical capability notice to
28 a designated communications provider unless:
29 (a) the Attorney-General is satisfied that the requirements
30 imposed by the notice are reasonable and proportionate; and
-

EXPOSURE DRAFT

Schedule 1 Industry assistance

- 1 (b) the Attorney-General is satisfied that compliance with the
2 notice is:
3 (i) practicable; and
4 (ii) technically feasible.

5 **317W Consultation about a proposal to give a technical capability** 6 **notice**

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

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

2 **317X Variation of technical capability notices**

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

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

7 (2) The acts or things specified in a varied technical capability notice
8 must be:

- 9 (a) in connection with any or all of the eligible activities of the
10 designated communications provider concerned; and
11 (b) covered by subsection 317T(2).

12 (3) The acts or things that may be specified in a varied technical
13 capability notice in accordance with paragraph 317T(2)(b) include
14 (but are not limited to) listed acts or things, so long as those acts or
15 things:

- 16 (a) are in connection with any or all of the eligible activities of
17 the designated communications provider concerned; and
18 (b) are covered by subsection 317T(2), so far as that subsection
19 relates to paragraph 317T(2)(b).

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

21 *Decision-making criteria*

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

EXPOSURE DRAFT

Schedule 1 Industry assistance

317Y Consultation about a proposal to vary a technical capability notice

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

15 **317ZA Compliance with notices—carriers and carriage service**
16 **providers**

- 17 (1) A carrier or carriage service provider must comply with a
18 requirement under:
- 19 (a) a technical assistance notice; or
- 20 (b) a technical capability notice;
- 21 to the extent that the carrier or provider is capable of doing so.
- 22 (2) A person must not:
- 23 (a) aid, abet, counsel or procure a contravention of
24 subsection (1); or
- 25 (b) induce, whether by threats or promises or otherwise, a
26 contravention of subsection (1); or
- 27 (c) be in any way, directly or indirectly, knowingly concerned in,
28 or party to, a contravention of subsection (1); or
- 29 (d) conspire with others to effect a contravention of
30 subsection (1).
- 31 (3) Subsections (1) and (2) are civil penalty provisions.

EXPOSURE DRAFT

Schedule 1 Industry assistance

1 Note: Part 31 provides for pecuniary penalties for breaches of civil penalty
2 provisions.

3 **317ZB Compliance with notices—designated communications**
4 **provider (other than a carrier or carriage service**
5 **provider)**

6 (1) A designated communications provider (other than a carrier or
7 carriage service provider) must comply with a requirement under:
8 (a) a technical assistance notice; or
9 (b) a technical capability notice;
10 to the extent that the provider is capable of doing so.

11 Civil penalty:
12 (a) if the provider is a body corporate—47,619 penalty units; or
13 (b) if the provider is not a body corporate—238 penalty units.

14 (2) The pecuniary penalty for a contravention by a designated
15 communications provider of subsection (1) must not be more than:
16 (a) if the provider is a body corporate—47,619 penalty units; or
17 (b) if the provider is not a body corporate—238 penalty units.

18 (3) Subsection 82(5) of the *Regulatory Powers (Standard Provisions)*
19 *Act 2014* does not apply to a contravention of subsection (1) of this
20 section.

21 (4) Sections 564 and 572B do not apply to a contravention of
22 subsection (1) of this section.

23 **317ZC Civil penalty provision**

24 *Enforceable civil penalty provision*

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

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

1 *Authorised applicant*

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

5 *Relevant courts*

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

10 *Extension to external Territories etc.*

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

15 **317ZD Enforceable undertakings**

16 *Enforceable provision*

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

19 *Authorised person*

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

23 *Relevant courts*

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

EXPOSURE DRAFT

Industry assistance **Schedule 1**

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

EXPOSURE DRAFT

EXPOSURE DRAFT

Schedule 1 Industry assistance

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

EXPOSURE DRAFT

Industry assistance **Schedule 1**

- 1 (vi) if the person is or was an arbitrator appointed under
2 section 317ZK—in the person’s capacity as such an
3 arbitrator.

4 Penalty: Imprisonment for 5 years.

5 *Exceptions*

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

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

10 *Authorised disclosures—general*

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

EXPOSURE DRAFT

Schedule 1 Industry assistance

- 1 (b) the *Regulatory Powers (Standard Provisions) Act 2014*, so
2 far as that Act relates to this Part.

3 *Authorised disclosures—IGIS official*

- 4 (5) An IGIS official may disclose:
5 (a) technical assistance notice information; or
6 (b) technical capability notice information; or
7 (c) technical assistance request information;
8 in connection with the IGIS official exercising powers, or
9 performing functions or duties, as an IGIS official.

10 *Authorised disclosures—information sharing*

- 11 (6) The Director-General of Security or the Communications Access
12 Co-ordinator may disclose information that is:
13 (a) technical assistance notice information; or
14 (b) technical capability notice information; or
15 (c) technical assistance request information;
16 to the chief officer of an interception agency for purposes relating
17 to the performance of functions, or the exercise of powers, by the
18 interception agency.

- 19 (7) The chief officer of an interception agency may disclose
20 information that is:
21 (a) technical assistance notice information; or
22 (b) technical capability notice information; or
23 (c) technical assistance request information;
24 to the chief officer of another interception agency for purposes
25 relating to the performance of functions, or the exercise of powers,
26 by the other interception agency.

- 27 (8) The Director-General of Security, the Director-General of the
28 Australian Signals Directorate or the chief officer of an
29 interception agency may disclose information that is:
30 (a) technical assistance notice information; or
31 (b) technical capability notice information; or
32 (c) technical assistance request information;

EXPOSURE DRAFT

Industry assistance **Schedule 1**

- 1 to the Director-General of the Australian Secret Intelligence
2 Service for purposes relating to the performance of functions, or
3 the exercise of powers, by the Australian Secret Intelligence
4 Service.
- 5 (9) The Director-General of Security, the Director-General of the
6 Australian Secret Intelligence Service or the chief officer of an
7 interception agency 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 Director-General of the Australian Signals Directorate for
12 purposes relating to the performance of functions, or the exercise
13 of powers, by the Australian Signals Directorate.
- 14 (10) The Communications Access Co-ordinator, the Director-General of
15 the Australian Secret Intelligence Service, the Director-General of
16 the Australian Signals Directorate 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 Director-General of Security for purposes relating to the
22 performance of functions, or the exercise of powers, by ASIO.
- 23 (11) The Director-General of Security 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 Communications Access Co-ordinator for purposes relating
29 to the performance of functions, or the exercise of powers, by the
30 Communications Access Co-ordinator.
- 31 (12) Before disclosing information under subsection (6), (7), (8), (9) or
32 (10), the Director-General of Security, the Director-General of the
33 Australian Secret Intelligence Service, the Director-General of the
34 Australian Signals Directorate or the chief officer of an

EXPOSURE DRAFT

EXPOSURE DRAFT

Schedule 1 Industry assistance

1 interception agency, as the case requires, must notify the
2 Communications Access Co-ordinator of the proposed disclosure.

3 *Authorised disclosures—statistics*

4 (13) A person who is:

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

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

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

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

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

23 **Division 7—Limitations**

24 **317ZG Designated communications provider must not be required** 25 **to implement or build a systemic weakness or systemic** 26 **vulnerability etc.**

27 (1) A technical assistance notice or technical capability notice must
28 not have the effect of:

- 29 (a) requiring a designated communications provider to
30 implement or build a systemic weakness, or a systemic
31 vulnerability, into a form of electronic protection; or

- 1 (b) preventing a designated communications provider from
2 rectifying a systemic weakness, or a systemic vulnerability,
3 in a form of electronic protection.
- 4 (2) The reference in paragraph (1)(a) to implement or build a systemic
5 weakness, or a systemic vulnerability, into a form of electronic
6 protection includes a reference to implement or build a new
7 decryption capability in relation to a form of electronic protection.
- 8 (3) The reference in paragraph (1)(a) to implement or build a systemic
9 weakness, or a systemic vulnerability, into a form of electronic
10 protection includes a reference to one or more actions that would
11 render systemic methods of authentication or encryption less
12 effective.
- 13 (4) Subsections (2) and (3) are enacted for the avoidance of doubt.
- 14 (5) A technical assistance notice or technical capability notice has no
15 effect to the extent (if any) to which it would have an effect
16 covered by paragraph (1)(a) or (b).

17 **317ZH General limits on technical assistance notices and technical**
18 **capability notices**

- 19 (1) A technical assistance notice or technical capability notice has no
20 effect to the extent (if any) to which it would require a designated
21 communications provider to do an act or thing for which a warrant
22 or authorisation under any of the following laws is required:
23 (a) the *Telecommunications (Interception and Access) Act 1979*;
24 (b) the *Surveillance Devices Act 2004*;
25 (c) the *Crimes Act 1914*;
26 (d) the *Australian Security Intelligence Organisation Act 1979*;
27 (e) the *Intelligence Services Act 2001*.
- 28 (2) For the purposes of subsection (1):
29 (a) assume that each law mentioned in that subsection applied
30 both within and outside Australia; and
31 (b) assume that each reference in Part 13 to a carriage service
32 provider included a reference to a designated
33 communications provider.

EXPOSURE DRAFT

Schedule 1 Industry assistance

- 1 (3) A technical assistance notice or technical capability notice has no
2 effect to the extent (if any) to which it would require a designated
3 communications provider to:
- 4 (a) use a surveillance device (within the meaning of the
5 *Surveillance Devices Act 2004*); or
6 (b) access data held in a computer (within the meaning of the
7 *Surveillance Devices Act 2004*);
- 8 if a law of a State or Territory requires a warrant or authorisation
9 for that use or access.
- 10 (4) To avoid doubt, subsection (1) or (3) does not prevent a technical
11 assistance notice or technical capability notice from requiring a
12 designated communications provider to do an act or thing by way
13 of giving help to:
- 14 (a) ASIO; or
15 (b) an interception agency;
- 16 in relation to:
- 17 (c) in the case of a technical assistance notice—a matter covered
18 by paragraph 317L(2)(c) or (d); or
19 (d) in the case of a technical capability notice—a matter covered
20 by subparagraph 317T(2)(b)(i) or (ii);
- 21 if the doing of the act or thing would:
- 22 (e) assist in, or facilitate, giving effect to a warrant or
23 authorisation under a law of the Commonwealth, a State or a
24 Territory; or
25 (f) give effect to a warrant or authorisation under a law of the
26 Commonwealth.
- 27 (5) To avoid doubt, subsection (1) or (3) does not prevent a technical
28 capability notice from requiring a designated communications
29 provider to do an act or thing directed towards ensuring that the
30 provider is capable of giving listed help (within the meaning of
31 section 317T) to:
- 32 (a) ASIO; or
33 (b) an interception agency;
- 34 in relation to a matter covered by subparagraph 317T(2)(a)(i) or
35 (ii), if the doing of the act or thing would:

- 1 (c) assist in, or facilitate, giving effect to a warrant or
2 authorisation under a law of the Commonwealth, a State or a
3 Territory; or
4 (d) give effect to a warrant or authorisation under a law of the
5 Commonwealth.

6 **Division 8—General provisions**

7 **317ZJ Immunity**

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

EXPOSURE DRAFT

Schedule 1 Industry assistance

1 **317ZK Terms and conditions on which help is to be given etc.**

2 *Scope*

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

EXPOSURE DRAFT

Industry assistance **Schedule 1**

1

Basis of compliance

2

- (3) The designated communications provider must comply with the requirement on the basis that the provider neither:

3

(a) profits from complying with the requirement; nor

4

5

(b) bears the reasonable costs of complying with the requirement;

6

7

unless the provider and the applicable costs negotiator otherwise agree.

8

9

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

10

Terms and conditions

11

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

12

13

(a) agreed between the following parties:

14

(i) the provider;

15

(ii) the applicable costs negotiator; or

16

(b) failing agreement, determined by an arbitrator appointed by the parties.

17

18

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

19

- (5) If:

20

(a) the parties fail to agree on the appointment of an arbitrator;

21

and

22

(b) one of the parties is a carrier or carriage service provider;

23

the ACMA is to appoint the arbitrator.

24

- (6) If:

25

(a) the parties fail to agree on the appointment of an arbitrator;

26

and

27

(b) none of the parties is a carrier or carriage service provider;

28

the Attorney-General is to appoint the arbitrator.

29

Arbitration

30

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

31

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

EXPOSURE DRAFT

Schedule 1 Industry assistance

- 1 (b) a person who belongs to a class of persons specified under
2 subsection (11).
- 3 (8) The Minister may, by writing, specify one or more persons for the
4 purposes of paragraph (7)(a).
- 5 (9) An instrument made under subsection (8) is not a legislative
6 instrument.
- 7 (10) Subsection 33(3AB) of the *Acts Interpretation Act 1901* does not
8 apply to the power conferred by subsection (8).
- 9 (11) The Minister may, by legislative instrument, specify a class of
10 persons for the purposes of paragraph (7)(b).
- 11 (12) Before making an instrument under subsection (8) or (11), the
12 Minister must consult the Attorney-General.
- 13 (13) If an arbitration under this section is conducted by an arbitrator
14 appointed by the ACMA, the cost of the arbitration must be
15 apportioned equally between the parties.
- 16 (14) The Minister may, by legislative instrument, make provision for
17 and in relation to the conduct of an arbitration under this section.

18 *Acquisition of property*

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

23 *Applicable costs negotiator*

- 24 (16) For the purposes of this section, the *applicable costs negotiator* is:
25 (a) in the case of a requirement under a technical assistance
26 notice given by the Director-General of Security—the
27 Director-General of Security; or
28 (b) in the case of a requirement under a technical assistance
29 notice given by the chief officer of an interception agency—
30 the chief officer; or

EXPOSURE DRAFT

Industry assistance **Schedule 1**

- 1 (c) in the case of a requirement under a technical capability
2 notice—the person specified in the notice, in accordance with
3 subsection 317T(12), as the applicable costs negotiator for
4 the notice.

5 **317ZL Service of notices etc.**

6 *Scope*

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

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

- 19 (2) If:
20 (a) the summons, process or notice, as the case may be, is
21 required to be served on, or given to, a designated
22 communications provider; and
23 (b) the designated communications provider has nominated an
24 address for service in a document given by the provider to:
25 (i) the Attorney-General; or
26 (ii) the Communications Access Co-ordinator; or
27 (iii) the Director-General of Security; or
28 (iv) the chief officer of an interception agency;
29 the summons, process, or notice, as the case may be, is taken to
30 have been served on, or given to, the provider if it is left at, or sent
31 by pre-paid post to, the nominated address for service.

- 32 (3) If:

EXPOSURE DRAFT

EXPOSURE DRAFT

Schedule 1 Industry assistance

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

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

- 15 (4) If:
16 (a) the summons, process or notice, as the case may be, is
17 required to be served on, or given to, a body corporate
18 incorporated outside Australia; and
19 (b) the body corporate does not have a registered office or a
20 principal office in Australia; and
21 (c) the body corporate has an agent in Australia;
22 the summons, process or notice, as the case may be, is taken to
23 have been served on, or given to, the body corporate if it is served
24 on, or given to, the agent.
- 25 (5) If:
26 (a) the summons, process or notice, as the case may be, is
27 required to be served on, or given to, a body corporate
28 incorporated outside Australia; and
29 (b) the body corporate does not have a registered office or a
30 principal office in Australia; and
31 (c) the body corporate carries on business, or conducts activities,
32 at an address in Australia;
33 the summons, process or notice, as the case may be, is taken to
34 have been served on, or given to, the body corporate if it is left at,
35 or sent by pre-paid post to, that address.

EXPOSURE DRAFT

Industry assistance **Schedule 1**

Other matters

(6) Subsections (2), (3), (4) and (5) have effect in addition to:

- (a) section 28A of the *Acts Interpretation Act 1901*; and
- (b) sections 587 and 588 of this Act.

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

317ZM Interception agency—chief officer and officer

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

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

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 Commissioner Act 2006</i>)
3	Australian Crime Commission	Chief Executive Officer of the Australian Crime	(a) the Chief Executive Officer of the Australian Crime

EXPOSURE DRAFT

Schedule 1 Industry assistance

Chief officer and officers of interception agencies			
Item	Column 1	Column 2	Column 3
	Interception agency	Chief officer	Officer
		Commission	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) of that Act
7	Law Enforcement Conduct Commission	the Chief Commissioner (within	(a) the Chief Commissioner (within the meaning
58	<i>Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018</i>		No. , 2018

EXPOSURE DRAFT

Industry assistance Schedule 1

Chief officer and officers of interception agencies			
Item	Column 1	Column 2	Column 3
	Interception agency	Chief officer	Officer
	of New South Wales	the meaning of the <i>Law Enforcement Conduct Commission Act 2016</i> (NSW))	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 <i>Crime and Corruption Act 2001</i> (Qld)) other than a person engaged

EXPOSURE DRAFT

Schedule 1 Industry assistance

Chief officer and officers of interception agencies			
Item	Column 1	Column 2	Column 3
	Interception agency	Chief officer	Officer
			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

EXPOSURE DRAFT

Schedule 1 Industry assistance

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

62 *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* No. , 2018

EXPOSURE DRAFT

Industry assistance Schedule 1

Potential delegates

Item	Column 1	Column 2
	Interception agency	Potential delegates
7	Law Enforcement Conduct Commission of New South Wales	(a) the Commissioner for Integrity (within the meaning 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

EXPOSURE DRAFT

Schedule 1 Industry assistance

1 occupies an office or position at an equivalent level to that of an
2 executive (within the meaning of the *Public Administration Act*
3 *2004* (Vic.)).

4 (5) For the purposes of this section, a person is at *executive level*, in
5 relation to an interception agency of South Australia, if the person
6 occupies an office or position at an equivalent level to that of an
7 executive employee (within the meaning of the *Public Sector Act*
8 *2009* (SA)).

9 **317ZS Annual reports**

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

24 **317ZT Alternative constitutional basis**

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

EXPOSURE DRAFT

Computer access warrants etc. **Schedule 2**
Amendments **Part 1**

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

EXPOSURE DRAFT

Schedule 2 Computer access warrants etc.

Part 1 Amendments

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

EXPOSURE DRAFT

Computer access warrants etc. **Schedule 2**
Amendments **Part 1**

- 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).

8 After subsection 27A(3B)

15 Insert:

- 16 (3C) If any thing has been done in relation to a computer under:
- 17 (a) a warrant under this section that authorises the Organisation
18 to do acts or things referred to in subsection 25A(4); or
19 (b) this subsection;
- 20 the Organisation is authorised to do 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) enter 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) enter any other premises for the purposes of gaining entry to
28 or exiting the premises referred to in paragraph (d);
- 29 (f) remove the computer or another thing from any place where
30 it is situated for the purposes of doing the things mentioned
31 in paragraph (c), and returning the computer or other thing to
32 that place;
33

EXPOSURE DRAFT

Schedule 2 Computer access warrants etc.

Part 1 Amendments

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

20 9 Paragraph 27E(2)(d)

21 Repeal the paragraph, substitute:

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

30 10 After paragraph 27E(2)(d)

31 Insert:

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

EXPOSURE DRAFT

Computer access warrants etc. **Schedule 2**
Amendments **Part 1**

1 **11 After paragraph 27E(2)(e)**

2 Insert:

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

6 **12 At the end of section 27E**

7 Add:

8 *Concealment of access etc.*

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

- 10 (a) a subsection (2) authorisation; or
11 (b) under this subsection;

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

13 (c) any thing reasonably necessary to conceal the fact that any
14 thing has been done under the subsection (2) authorisation or
15 under this subsection;

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

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

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

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

- 28 (i) use any other computer or a communication in transit to
29 do those things; and
30 (ii) if necessary to achieve that purpose—add, copy, delete
31 or alter other data in the computer or the communication
32 in transit;

EXPOSURE DRAFT

Schedule 2 Computer access warrants etc.

Part 1 Amendments

- 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 authorisation is in force or within 28
7 days 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 **13 Subsection 33(1)**

13 Repeal the subsection.

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

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

16 **15 Paragraph 34(2)(b)**

17 After “27E(2)”, insert “or (6)”.

18 **16 At the end of section 34**

19 Add:

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

EXPOSURE DRAFT

Computer access warrants etc. **Schedule 2**
Amendments **Part 1**

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

3 Before “26B(5)”, insert “25A(8)”.

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

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

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

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

9 After “44(1)(a)”, insert “(aa)”.

10 **26 After Part IIIA**

11 Insert:

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

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

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

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

EXPOSURE DRAFT

Schedule 2 Computer access warrants etc.

Part 1 Amendments

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

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

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

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

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

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

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

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

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

28 (a) a particular computer;

29 (b) a computer on particular premises;

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

32 (3) In this section:

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

EXPOSURE DRAFT

Computer access warrants etc. **Schedule 2**
Amendments **Part 1**

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

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

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

9 *Surveillance Devices Act 2004*

10 **27 Title**

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

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

13 Insert:

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

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

21 Insert:

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

EXPOSURE DRAFT

Schedule 2 Computer access warrants etc.

Part 1 Amendments

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

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

5 Insert:

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

10 **31 Paragraph 3(c)**

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

13 **32 Subsection 4(1)**

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

15 that:

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

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

19 Insert:

- 20 (4A) For the avoidance of doubt, it is intended that a warrant may be
21 issued, or an emergency authorisation given, under this Act:
22 (a) for access to data held in a computer; and
23 (b) in relation to a relevant offence or a recovery order.

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

25 Insert:

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

EXPOSURE DRAFT

Computer access warrants etc. **Schedule 2**
Amendments **Part 1**

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

7 **35 Subsection 6(1)**

8 Insert:

9 **carrier** means:

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

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

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

17 Repeal the definition, substitute:

18 **computer** means all or part of:

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

23 **37 Subsection 6(1)**

24 Insert:

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

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

29 **data** includes:

- 30 (a) information in any form; and

EXPOSURE DRAFT

Schedule 2 Computer access warrants etc.

Part 1 Amendments

1 (b) any program (or part of a program).

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

3 (a) data held in any removable data storage device for the time
4 being held in a computer; and

5 (b) data held in a data storage device on a computer network of
6 which the computer forms a part.

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

11 **38 Subsection 6(1) (definition of *data surveillance device*)**

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

14 **39 Subsection 6(1)**

15 Insert:

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

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

22 **40 Subsection 6(1) (definition of *mutual assistance*** 23 ***application*)**

24 Repeal the definition, substitute:

25 ***mutual assistance application*** means:

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

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

28 made under a mutual assistance authorisation.

EXPOSURE DRAFT

Computer access warrants etc. **Schedule 2**
Amendments **Part 1**

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

3 Omit “subsection 15CA(1)”, substitute, “subsection 15CA(1) or
4 15CC(1)”.

5 **42 Subsection 6(1) (paragraph (db) of the definition of**
6 ***relevant offence*)**

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

8 **43 Subsection 6(1) (definition of *remote application*)**

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

10 **44 Subsection 6(1)**

11 Insert:

12 *telecommunications facility* means a facility within the meaning of
13 the *Telecommunications Act 1997*.

14 **45 Subsection 6(1) (definition of *unsworn application*)**

15 Omit “or 22(4) and (5)”, substitute “, 22(4) and (5), 27A(9) and (10),
16 27A(11) and (12) or 27A(13) and (14)”.

17 **46 Subsection 6(1) (definition of *warrant*)**

18 Repeal the definition, substitute:

19 *warrant* means:

- 20 (a) a surveillance device warrant; or
21 (b) a retrieval warrant; or
22 (c) a computer access warrant.

23 **47 At the end of subsection 10(1)**

24 Add:

25 ; (c) a computer access warrant.

26 **48 Subsection 10(2)**

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

EXPOSURE DRAFT

Schedule 2 Computer access warrants etc.

Part 1 Amendments

1 **49 At the end of Part 2**

2 Add:

3 **Division 4—Computer access warrants**

4 **27A Application for computer access warrant**

5 *Warrants sought for offence investigations*

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

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

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

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

17 (i) the commission of those offences; or

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

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

23 *Warrants sought for recovery orders*

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

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

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

EXPOSURE DRAFT

Computer access warrants etc. **Schedule 2**
Amendments **Part 1**

1

Warrants sought for mutual assistance investigations

2

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

3

4

5

(a) is authorised to do so under a mutual assistance authorisation; and

6

7

(b) suspects on reasonable grounds that access to data held in a computer (the *target computer*) is necessary, in the course of the investigation or investigative proceeding to which the authorisation relates, for the purpose of enabling evidence to be obtained of:

8

9

10

11

12

(i) the commission of the offence to which the authorisation relates; or

13

14

(ii) the identity or location of the persons suspected of committing the offence.

15

16

Warrants sought for integrity operations

17

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

18

19

20

(a) an integrity authority is in effect authorising an integrity operation in relation to an offence that it is suspected has been, is being or is likely to be committed by a staff member of a target agency; and

21

22

23

24

(b) the federal law enforcement officer suspects on reasonable grounds that access to data held in a computer (the *target computer*) will assist the conduct of the integrity operation by enabling evidence to be obtained relating to the integrity, location or identity of any staff member of the target agency.

25

26

27

28

29

Control order access warrants

30

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

31

32

33

(a) a control order is in force in relation to a person; and

EXPOSURE DRAFT

Schedule 2 Computer access warrants etc.

Part 1 Amendments

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

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

16 *Procedure for making applications*

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

25 *Unsworn applications—warrants sought for offence investigations*

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

EXPOSURE DRAFT

Computer access warrants etc. **Schedule 2**
Amendments **Part 1**

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

9 *Unsworn applications—warrants sought for recovery orders*

- 10 (11) If a law enforcement officer believes that:
11 (a) immediate access to data held in the target computer referred
12 to in subsection (3) may assist as described in
13 paragraph (3)(b); and
14 (b) it is impracticable for an affidavit to be prepared or sworn
15 before an application for a warrant is made;
16 an application for a warrant under subsection (3) may be made
17 before an affidavit is prepared or sworn.

- 18 (12) If subsection (11) applies, the applicant must:
19 (a) provide as much information as the eligible Judge or
20 nominated AAT member considers is reasonably practicable
21 in the circumstances; and
22 (b) not later than 72 hours after the making of the application,
23 send a duly sworn affidavit to the eligible Judge or
24 nominated AAT member, whether or not a warrant has been
25 issued.

26 *Unsworn applications—control order access warrants*

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

EXPOSURE DRAFT

Schedule 2 Computer access warrants etc.

Part 1 Amendments

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

9 *Target computer*

- 10 (15) The target computer referred to in subsection (1), (3), (4), (5) or (6)
11 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 **27B Remote application**

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

25 **27C Determining the application**

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

EXPOSURE DRAFT

Computer access warrants etc. **Schedule 2**
Amendments **Part 1**

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

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

- 34 (2) In determining whether a computer access warrant should be
35 issued, the eligible Judge or nominated AAT member must have
36 regard to:

EXPOSURE DRAFT

Schedule 2 Computer access warrants etc.

Part 1 Amendments

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

EXPOSURE DRAFT

Computer access warrants etc. **Schedule 2**
Amendments **Part 1**

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

31 **27D What must a computer access warrant contain?**

- 32 (1) A computer access warrant must:
- 33 (a) state that the eligible Judge or nominated AAT member
34 issuing the warrant is satisfied of the matters referred to in
35 subsection 27C(1) and has had regard to the matters referred
36 to in subsection 27C(2); and

EXPOSURE DRAFT

Schedule 2 Computer access warrants etc.

Part 1 Amendments

- 1 (b) specify:
- 2 (i) the name of the applicant; and
- 3 (ii) if the warrant relates to one or more alleged relevant
- 4 offences—the alleged offences in respect of which the
- 5 warrant is issued; and
- 6 (iii) if the warrant relates to a recovery order—the date the
- 7 order was made and the name of the child to whom the
- 8 order relates; and
- 9 (iv) if the warrant relates to a mutual assistance
- 10 authorisation—the offence or offences against the law
- 11 of a foreign country to which the authorisation relates;
- 12 and
- 13 (v) if the warrant is issued for the purposes of an integrity
- 14 operation—the integrity authority for the operation and
- 15 each alleged relevant offence in relation to which the
- 16 authority was granted; and
- 17 (vi) the date the warrant is issued; and
- 18 (vii) if the target computer is or includes a particular
- 19 computer—the computer; and
- 20 (viii) if the target computer is or includes a computer on
- 21 particular premises—the premises; and
- 22 (ix) if the target computer is or includes a computer
- 23 associated with, used by or likely to be used by, a
- 24 person—the person (whether by name or otherwise);
- 25 and
- 26 (x) the period during which the warrant is in force (see
- 27 subsection (3)); and
- 28 (xi) the name of the law enforcement officer primarily
- 29 responsible for executing the warrant.
- 30 (2) If a control order access warrant is issued on the basis of a control
- 31 order that is in force in relation to a person, the warrant must also
- 32 specify the following details in relation to the control order:
- 33 (a) the name of the person;
- 34 (b) the date the control order was made;
- 35 (c) whether the control order is an interim control order or a
- 36 confirmed control order.

EXPOSURE DRAFT

Computer access warrants etc. **Schedule 2**
Amendments **Part 1**

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

21 **27E What a computer access warrant authorises**

- 22 (1) A computer access warrant must authorise the doing of specified
23 things (subject to any restrictions or conditions specified in the
24 warrant) in relation to the relevant target computer.
- 25 (2) The things that may be specified are any of the following that the
26 eligible Judge or nominated AAT member considers appropriate in
27 the circumstances:
28 (a) entering specified premises for the purposes of doing the
29 things mentioned in this subsection;
30 (b) entering any premises for the purposes of gaining entry to, or
31 exiting, the specified premises;
32 (c) using:
33 (i) the target computer; or

EXPOSURE DRAFT

Schedule 2 Computer access warrants etc.

Part 1 Amendments

- 1 (ii) a telecommunications facility operated or provided by
2 the Commonwealth or a carrier; or
3 (iii) any other electronic equipment; or
4 (iv) a data storage device;
5 for the purpose of obtaining access to data (the *relevant data*)
6 that is held in the target computer at any time while the
7 warrant is in force, in order to determine whether the relevant
8 data is covered by the warrant;
- 9 (d) if necessary to achieve the purpose mentioned in
10 paragraph (c)—adding, copying, deleting or altering other
11 data in the target computer;
- 12 (e) if, having regard to other methods (if any) of obtaining access
13 to the relevant data which are likely to be as effective, it is
14 reasonable in all the circumstances to do so:
- 15 (i) using any other computer or a communication in transit
16 to access the relevant data; and
17 (ii) if necessary to achieve that purpose—adding, copying,
18 deleting or altering other data in the computer or the
19 communication in transit;
- 20 (f) removing a computer or other thing from premises for the
21 purposes of doing any thing specified in the warrant in
22 accordance with this subsection, and returning the computer
23 or other thing to the premises;
- 24 (g) copying any data to which access has been obtained, and that:
25 (i) appears to be relevant for the purposes of determining
26 whether the relevant data is covered by the warrant; or
27 (ii) is covered by the warrant;
- 28 (h) intercepting a communication passing over a
29 telecommunications system, if the interception is for the
30 purposes of doing any thing specified in the warrant in
31 accordance with this subsection;
- 32 (i) any other thing reasonably incidental to any of the above.
- 33 Note: As a result of the warrant, a person who, by means of a
34 telecommunications facility, obtains access to data stored in a
35 computer etc. will not commit an offence under Part 10.7 of the
36 *Criminal Code* or equivalent State or Territory laws (provided that the
37 person acts within the authority of the warrant).
-

EXPOSURE DRAFT

Computer access warrants etc. **Schedule 2**
Amendments **Part 1**

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

6 *When data is covered by a warrant*

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

23 *Certain acts not authorised*

- 24 (5) Subsection (2) does 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 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.

EXPOSURE DRAFT

Schedule 2 Computer access warrants etc.

Part 1 Amendments

1 *Warrant must provide for certain matters*

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

9 *Concealment of access etc.*

- 10 (7) If any thing has been done in relation to a computer under:
- 11 (a) a computer access warrant; or
- 12 (b) this subsection;
- 13 then, in addition to the things specified in the warrant, the warrant
- 14 authorises the doing of any of the following:
- 15 (c) any thing reasonably necessary to conceal the fact that any
- 16 thing has been done under the warrant or under this
- 17 subsection;
- 18 (d) entering any premises where the computer is reasonably
- 19 believed to be, for the purposes of doing the things
- 20 mentioned in paragraph (c);
- 21 (e) entering any other premises for the purposes of gaining entry
- 22 to or exiting the premises referred to in paragraph (d);
- 23 (f) removing the computer or another thing from any place
- 24 where it is situated for the purposes of doing the things
- 25 mentioned in paragraph (c), and returning the computer or
- 26 other thing to that place;
- 27 (g) if, having regard to other methods (if any) of doing the things
- 28 mentioned in paragraph (c) which are likely to be as
- 29 effective, it is reasonable in all the circumstances to do so:
- 30 (i) using any other computer or a communication in transit
- 31 to do those things; and
- 32 (ii) if necessary to achieve that purpose—adding, copying,
- 33 deleting or altering other data in the computer or the
- 34 communication in transit;

EXPOSURE DRAFT

Computer access warrants etc. **Schedule 2**
Amendments **Part 1**

- 1 (h) intercepting 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 **27F Extension and variation of computer access warrant**

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

EXPOSURE DRAFT

Schedule 2 Computer access warrants etc.

Part 1 Amendments

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

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

6 **27G Revocation of computer access warrant**

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

12 (2) If the circumstances set out in paragraphs 27H(2)(a) and (b),
13 27H(3)(a) and (b), 27H(4)(a) and (b), 27H(5)(a) and (b), 27H(6)(a)
14 and (b) or 27H(7)(a) and (b) apply in relation to a computer access
15 warrant, the chief officer of the law enforcement agency to which
16 the law enforcement officer to whom the warrant was issued
17 belongs or is seconded must, by instrument in writing, revoke the
18 warrant.

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

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

27 (5) If:

28 (a) an eligible Judge or nominated AAT member revokes a
29 warrant; and

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

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

EXPOSURE DRAFT

27H Discontinuance of access under warrant

2 *Scope*

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

5 *Discontinuance of access*

6 (2) If:

7 (a) the computer access warrant has been sought by or on behalf
8 of a law enforcement officer in relation to a relevant offence;

9 and

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

14 (i) the commission of the relevant offence; or

15 (ii) the identity or location of the offender;

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

19 (3) If:

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

22 and

23 (b) the chief officer of the law enforcement agency to which the
24 law enforcement officer belongs or is seconded is satisfied
25 that access to data under the warrant is no longer required for
26 the purpose of locating and safely recovering the child to
27 whom the recovery order relates;

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

31 (4) If:

EXPOSURE DRAFT

Schedule 2 Computer access warrants etc.

Part 1 Amendments

- 1 (a) the computer access warrant has been sought by or on behalf
2 of a law enforcement officer as authorised under a mutual
3 assistance authorisation; and
4 (b) the chief officer of the law enforcement agency to which the
5 law enforcement officer belongs or is seconded is satisfied
6 that access to data under the warrant is no longer required for
7 the purpose of enabling evidence to be obtained of:
8 (i) the commission of the offence against a law of a foreign
9 country to which the authorisation relates; or
10 (ii) the identity or location of the persons suspected of
11 committing the offence;

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.

15 (5) If:

- 16 (a) the computer access warrant has been sought by or on behalf
17 of a federal law enforcement officer for the purposes of an
18 integrity operation; and
19 (b) the chief officer of the law enforcement agency to which the
20 law enforcement officer belongs or is seconded is satisfied
21 that:
22 (i) access to data under the warrant is no longer necessary
23 for the purposes of the integrity operation; or
24 (ii) the integrity authority for the integrity operation is no
25 longer in effect;

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

29 (6) If:

- 30 (a) the computer access warrant is a control order access warrant
31 issued on the basis of a control order that was in force in
32 relation to a person; and
33 (b) the chief officer of the law enforcement agency to which the
34 law enforcement officer belongs or is seconded is satisfied
35 that access to data under the warrant to obtain information

EXPOSURE DRAFT

Computer access warrants etc. **Schedule 2**
Amendments **Part 1**

- 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

EXPOSURE DRAFT

Schedule 2 Computer access warrants etc.

Part 1 Amendments

- 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.

50 After subsection 28(1)

24
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

EXPOSURE DRAFT

Computer access warrants etc. **Schedule 2**
Amendments **Part 1**

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)”.

EXPOSURE DRAFT

Schedule 2 Computer access warrants etc.

Part 1 Amendments

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

2 Insert:

3 (1A) If:

4 (a) a law enforcement officer is conducting an investigation into:

5 (i) an offence against section 233BAA of the *Customs Act*
6 *1901* (with respect to goods listed in Schedule 4 to the
7 *Customs (Prohibited Imports) Regulations 1956* or in
8 Schedule 8 or 9 to the *Customs (Prohibited Exports)*
9 *Regulations 1958*); or

10 (ii) an offence under the *Crimes (Traffic in Narcotic Drugs*
11 *and Psychotropic Substances) Act 1990* or an offence
12 against Part 9.1 of the *Criminal Code* (other than
13 section 308.1 or 308.2); or

14 (iii) an offence against section 73.2 or 73.3 or Division 91 of
15 the *Criminal Code*; or

16 (iv) an offence under Subdivision A of Division 72 or
17 Division 80, 101, 102, 103, 270, 272 or 273 of the
18 *Criminal Code*; or

19 (v) an offence against section 233B or 233C of the
20 *Migration Act 1958*;

21 or more than one offence; and

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

23 (i) access to data held in a computer (the **target computer**)
24 is immediately necessary to prevent the loss of any
25 evidence relevant to that investigation; and

26 (ii) the circumstances are so serious and the matter is of
27 such urgency that access to data held in the target
28 computer is warranted; and

29 (iii) it is not practicable in the circumstances to apply for a
30 computer access warrant;

31 the law enforcement officer may apply to an appropriate
32 authorising officer for an emergency authorisation for access to
33 data held in the target computer.

34 (1B) The target computer may be any one or more of the following:

35 (a) a particular computer;

EXPOSURE DRAFT

Computer access warrants etc. **Schedule 2**
Amendments **Part 1**

- 1 (b) a computer on particular premises;
2 (c) a computer associated with, used by or likely to be used by, a
3 person (whose identity may or may not be known).

4 **55 Subsection 30(2)**

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

6 **56 Subsection 30(3)**

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

9 **57 At the end of section 30**

10 Add:

- 11 (4) In the case of an application mentioned in subsection (1A), the
12 appropriate authorising officer may give the emergency
13 authorisation if satisfied that:
14 (a) an investigation is being conducted into an offence referred
15 to in paragraph (1A)(a); and
16 (b) there are reasonable grounds for the suspicion referred to in
17 paragraph (1A)(b).

18 **58 Subsections 32(1) and (2)**

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

20 **59 After subsection 32(2)**

21 Insert:

- 22 (2A) An emergency authorisation for access to data held in a computer
23 may authorise anything that a computer access warrant may
24 authorise.

25 **60 After subsection 32(3)**

26 Insert:

- 27 (3A) A law enforcement officer may, under an emergency authorisation,
28 access data held in a computer only if the officer is acting in the
29 performance of the officer’s duty.

EXPOSURE DRAFT

Schedule 2 Computer access warrants etc.

Part 1 Amendments

1 **61 Subsection 33(2)**

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

4 **62 After subsection 33(2)**

5 Insert:

6 (2A) In the case of an application for an emergency authorisation for
7 access to data held in a computer, the application:

8 (a) must specify:

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

10 (ii) if a warrant is sought—the nature and duration of the
11 warrant; and

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

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

16 **63 Subsection 34(1)**

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

18 **64 After subsection 34(1)**

19 Insert:

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

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

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

30 (c) the extent to which law enforcement officers could have used
31 alternative methods of investigation to help reduce or avoid
32 the risk;

EXPOSURE DRAFT

Computer access warrants etc. **Schedule 2**
Amendments **Part 1**

- 1 (d) how much the use of alternative methods of investigation
2 could have helped reduce or avoid the risk;
3 (e) how much the use of alternative methods of investigation
4 would have prejudiced the safety of the person or property
5 because of delay or for another reason;
6 (f) whether or not it was practicable in the circumstances to
7 apply for a computer access warrant.

8 **65 Subsection 34(2)**

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

10 **66 After subsection 34(2)**

11 Insert:

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

30 **67 Subsection 34(3)**

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

32 **68 At the end of section 34**

33 Add:

EXPOSURE DRAFT

Schedule 2 Computer access warrants etc.

Part 1 Amendments

- 1 (4) Before deciding an application for approval of the giving of an
2 emergency authorisation given in response to an application under
3 subsection 30(1A), the eligible Judge or nominated AAT member
4 must, in particular, and being mindful of the intrusive nature of
5 accessing data held in the target computer mentioned in that
6 subsection, consider the following:
7 (a) the nature of the risk of the loss of evidence;
8 (b) the extent to which issuing a computer access warrant would
9 have helped reduce or avoid the risk;
10 (c) the extent to which law enforcement officers could have used
11 alternative methods of investigation to help reduce or avoid
12 the risk;
13 (d) how much the use of alternative methods of investigation
14 could have helped reduce or avoid the risk;
15 (e) whether or not it was practicable in the circumstances to
16 apply for a computer access warrant.

17 **69 Section 35 (heading)**

18 Repeal the heading, substitute:

19 **35 Judge or nominated AAT member may approve giving of an**
20 **emergency authorisation for the use of a surveillance**
21 **device**

22 **70 Subsection 35(1)**

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

25 **71 Subsection 35(1)**

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

27 **72 Subsection 35(2)**

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

30 **73 Subsection 35(2)**

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

EXPOSURE DRAFT

Computer access warrants etc. **Schedule 2**
Amendments **Part 1**

1 **74 Subsection 35(3)**

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

4 **75 Subsection 35(3)**

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

6 **76 After section 35**

7 Insert:

8 **35A Judge or nominated AAT member may approve giving of an**
9 **emergency authorisation for access to data held in a**
10 **computer**

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

EXPOSURE DRAFT

Schedule 2 Computer access warrants etc.

Part 1 Amendments

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

EXPOSURE DRAFT

Computer access warrants etc. **Schedule 2**
Amendments **Part 1**

1 of Part 2 is currently justified—issue a computer access
2 warrant relating to the subsequent access to such data as if
3 the application for the approval were an application for a
4 computer access warrant under Division 4 of Part 2.

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

11 **77 Section 36**

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

13 **78 Section 41 (definition of *appropriate consenting official*)**

14 Repeal the definition, substitute:

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

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

24 **79 Section 42 (heading)**

25 Repeal the heading, substitute:

26 **42 Extraterritorial operation of surveillance device warrants**

27 **80 Subsection 42(1)**

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

29 **81 After paragraph 42(2)(a)**

30 Insert:

EXPOSURE DRAFT

Schedule 2 Computer access warrants etc.

Part 1 Amendments

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

3 **82 Paragraph 42(2)(b)**

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

5 **83 Subsection 42(2)**

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

7 **84 Subsection 42(2)**

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

9 **85 Paragraph 42(3)(a)**

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

11 **86 Subsections 42(6) and (9)**

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

13 **87 At the end of Part 5**

14 Add:

15 **43A Extraterritorial operation of computer access warrants**

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

21 (a) in a foreign country; or

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

25 to assist in that investigation, the eligible Judge or nominated AAT
26 member considering the application for the warrant must not
27 permit the warrant to authorise that access unless the eligible Judge
28 or nominated AAT member is satisfied that the access has been

EXPOSURE DRAFT

Computer access warrants etc. **Schedule 2**
Amendments **Part 1**

1 agreed to by an appropriate consenting official of the foreign
2 country.

3 (2) If:

- 4 (a) application is made under section 33 by an appropriate
5 authorising officer who is a federal law enforcement officer
6 for approval of the giving of an emergency authorisation
7 relating to the investigation of a relevant offence; and
8 (b) the emergency authorisation was given in response to an
9 application under subsection 28(1A); and
10 (c) before the completion of consideration of that section 33
11 application, it becomes apparent to the applicant that there
12 will be a need for access to data held in a computer:
13 (i) in a foreign country; or
14 (ii) on a vessel or aircraft that is registered under the law of
15 a foreign country and is in or above waters beyond the
16 outer limits of the territorial sea of Australia;
17 to assist in the investigation to which the emergency
18 authorisation related;

19 the eligible Judge or nominated AAT member to whom the
20 section 33 application was made must not permit any computer
21 access warrant issued on consideration of that section 33
22 application to authorise that access unless the eligible Judge or
23 nominated AAT member is satisfied that the access has been
24 agreed to by an appropriate consenting official of the foreign
25 country.

26 (3) If:

- 27 (a) a computer access warrant has been issued in relation to the
28 investigation of a relevant offence in response to an
29 application by or on behalf of a federal law enforcement
30 officer; and
31 (b) after the issue of the warrant, it becomes apparent to the law
32 enforcement officer primarily responsible for executing the
33 warrant that there will be a need for access to data held in a
34 computer that is:
35 (i) in a foreign country; or

EXPOSURE DRAFT

Schedule 2 Computer access warrants etc.

Part 1 Amendments

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

EXPOSURE DRAFT

Computer access warrants etc. **Schedule 2**
Amendments **Part 1**

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

there is no requirement for the agreement of an appropriate consenting official of the foreign country concerned in relation to that access while the vessel is in those waters.

(7) As soon as practicable after the commencement of access to data held in a computer under the authority of a computer access warrant in circumstances where consent to that access is required:

(a) in a foreign country; or

(b) on a vessel or aircraft that is registered under the law of a foreign country;

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

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

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

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

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

Evidence obtained from access to data held in a computer undertaken in a foreign country in accordance with subsection 43A(1), (2) or (3) in relation to a relevant offence

EXPOSURE DRAFT

Schedule 2 Computer access warrants etc.

Part 1 Amendments

1 cannot be tendered in evidence to a court in any proceedings
2 relating to the relevant offence unless the court is satisfied that the
3 access was agreed to by an appropriate consenting official of the
4 foreign country.

5 **88 Subsection 44(1) (after paragraph (a) of the definition of**
6 ***protected information*)**

7 Insert:

- 8 (aa) any information (other than general computer access
9 intercept information) obtained from access to data under:
10 (i) a computer access warrant; or
11 (ii) an emergency authorisation for access to data held in a
12 computer; or

13 **90 Subsection 44(1) (at the end of subparagraph (d)(iii) of the**
14 **definition of *protected information*)**

15 Add “or”.

16 **91 Subsection 44(1) (after subparagraph (d)(iii) of the**
17 **definition of *protected information*)**

18 Insert:

- 19 (iv) in a case where the information was obtained through
20 access to data held in a computer in a foreign country,
21 or on a vessel or aircraft that is registered under the law
22 of a foreign country and that is in or above waters
23 beyond the outer limit of Australia’s territorial sea—
24 without the agreement of the appropriate consenting
25 official of that foreign country, and of any other foreign
26 country, whose agreement is required under
27 section 43A;

28 **91A Subsection 44(1) (at the end of the definition of**
29 ***protected information*)**

30 Add:

- 31 Note: For protection of general computer access intercept information, see
32 Part 2-6 of the *Telecommunications (Interception and Access) Act*
33 *1979*.

EXPOSURE DRAFT

Computer access warrants etc. **Schedule 2**
Amendments **Part 1**

1 **92 Section 46 (heading)**

2 Repeal the heading, substitute:

3 **46 Dealing with records obtained by using a surveillance device or**
4 **accessing data held in a computer**

5 **93 Paragraph 46(1)(a)**

6 After “protected information”, insert “or general computer access
7 intercept information”.

8 **94 Subsection 46(2)**

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

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

- 16 (aa) using a surveillance device; or
17 (ab) accessing data held in a computer;
18 the officer in charge of the agency:

19 **95 After subsection 46A(1)**

20 Insert:

21 (1A) If:

- 22 (a) a record or report is in the possession of a law enforcement
23 agency; and
24 (b) the record or report comprises information obtained from
25 access to data under a control order access warrant issued on
26 the basis of a control order made in relation to a person; and
27 (c) the warrant was issued for the purpose, or for purposes that
28 include the purpose, of obtaining information that would be
29 likely to substantially assist in connection with determining
30 whether the control order, or any succeeding control order,
31 has been, or is being, complied with; and

EXPOSURE DRAFT

Schedule 2 Computer access warrants etc.

Part 1 Amendments

- 1 (d) access to the data occurred when the control order had been
2 made, but had not come into force because it had not been
3 served on the person; and
4 (e) the chief officer of the agency is satisfied that none of the
5 information obtained from accessing the data is likely to
6 assist in connection with:
7 (i) the protection of the public from a terrorist act; or
8 (ii) preventing the provision of support for, or the
9 facilitation of, a terrorist act; or
10 (iii) preventing the provision of support for, or the
11 facilitation of, the engagement in a hostile activity in a
12 foreign country;
13 the chief officer of the agency must cause the record or report to be
14 destroyed as soon as practicable.

96 Subsection 46A(2)

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

97 After section 47

17 Insert:
18

47A Protection of computer access technologies and methods

- 19
20 (1) In a proceeding, a person may object to the disclosure of
21 information on the ground that the information, if disclosed, could
22 reasonably be expected to reveal details of computer access
23 technologies or methods.
24 (2) If the person conducting or presiding over the proceeding is
25 satisfied that the ground of objection is made out, the person may
26 order that the person who has the information not be required to
27 disclose it in the proceeding.
28 (3) In determining whether or not to make an order under
29 subsection (2), the person conducting or presiding over the
30 proceeding must take into account whether disclosure of the
31 information:
32 (a) is necessary for the fair trial of the defendant; or

EXPOSURE DRAFT

Computer access warrants etc. **Schedule 2**
Amendments **Part 1**

- 1 (b) is in the public interest.
- 2 (4) Subsection (2) does not affect a provision of another law under
3 which a law enforcement officer cannot be compelled to disclose
4 information or make statements in relation to the information.
- 5 (5) If the person conducting or presiding over a proceeding is satisfied
6 that publication of any information disclosed in the proceeding
7 could reasonably be expected to reveal details of computer access
8 technologies or methods, the person must make any orders
9 prohibiting or restricting publication of the information that the
10 person considers necessary to ensure that those details are not
11 revealed.
- 12 (6) Subsection (5) does not apply to the extent that the person
13 conducting or presiding over the proceeding considers that the
14 interests of justice require otherwise.
- 15 (7) In this section:
- 16 ***computer access technologies or methods*** means:
- 17 (a) technologies or methods relating to the use of:
- 18 (i) a computer; or
19 (ii) a telecommunications facility operated or provided by
20 the Commonwealth or a carrier; or
21 (iii) any other electronic equipment; or
22 (iv) a data storage device;
23 for the purpose of obtaining access to data held in the
24 computer; or
- 25 (b) technologies or methods relating to adding, copying, deleting
26 or altering other data in a computer, if doing so is necessary
27 to achieve the purpose mentioned in paragraph (a);
28 where the technologies or methods have been, or are being,
29 deployed in giving effect to:
- 30 (c) a computer access warrant; or
31 (d) an emergency authorisation given in response to an
32 application under subsection 28(1A), 29(1A) or 30(1A).
- 33 ***proceeding*** includes a proceeding before a court, tribunal or Royal
34 Commission.
-

EXPOSURE DRAFT

Schedule 2 Computer access warrants etc.

Part 1 Amendments

1 **98 Subsection 49(2)**

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

5 **99 After subsection 49(2A)**

6 Insert:

7 (2B) In the case of a computer access warrant, or an emergency
8 authorisation, for access to data held in a computer, the report
9 must:

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

11 (b) if so:

12 (i) state the name of the person primarily responsible for
13 the execution of the warrant or authorisation; and

14 (ii) state the name of each person involved in accessing data
15 under the warrant or authorisation; and

16 (iii) state the period during which the data was accessed; and

17 (iv) state the name, if known, of any person whose data was
18 accessed; and

19 (v) give details of any premises at which the computer was
20 located; and

21 (vi) if the warrant is issued, or the authorisation is given, in
22 respect of the investigation of a relevant offence—give
23 details of the benefit to the investigation of the accessed
24 data and of the general use made, or to be made, of any
25 evidence or information obtained by the access to data;
26 and

27 (vii) if the warrant is issued, or the authorisation is given, in
28 respect of the location and safe recovery of a child to
29 whom a recovery order relates—give details of the use
30 of the accessed data in assisting with the location and
31 safe recovery of the child; and

32 (viii) if the warrant is issued, or the authorisation is given, for
33 the purposes of an integrity operation—give details of
34 the benefit to the operation of the accessed data and of

EXPOSURE DRAFT

Computer access warrants etc. **Schedule 2**
Amendments **Part 1**

- 1 the general use made, or to be made, of any evidence or
2 information obtained by the access to data; and
3 (ix) if the warrant is a control order access warrant—give
4 the details specified in subsection (2C); and
5 (x) give details of the communication of evidence or
6 information obtained by access to data held in the
7 computer to persons other than officers of the agency;
8 and
9 (xi) give details of the compliance with the conditions (if
10 any) to which the warrant or authorisation was subject;
11 and
12 (c) if the warrant or authorisation was extended or varied, state:
13 (i) the number of extensions or variations; and
14 (ii) the reasons for them.
- 15 (2C) For the purposes of subparagraph (2B)(b)(ix), the details are:
16 (a) the benefit of obtaining access to data held in the computer
17 in:
18 (i) protecting the public from a terrorist act; or
19 (ii) preventing the provision of support for, or the
20 facilitation of, a terrorist act; or
21 (iii) preventing the provision of support for, or the
22 facilitation of, the engagement in a hostile activity in a
23 foreign country; or
24 (iv) determining whether a control order has been, or is
25 being, complied with; and
26 (b) the general use to be made of any evidence or information
27 obtained by access to data held in the computer.

28 **100 Subsection 49A(1)**

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

30 **101 Paragraph 49A(2)(a)**

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

32 **102 After paragraph 49A(2)(b)**

33 Insert:

EXPOSURE DRAFT

Schedule 2 Computer access warrants etc.

Part 1 Amendments

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

3 **103 After paragraph 49A(2)(c)**

4 Insert:

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

8 **104 Subsection 49A(3)**

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

10 **105 Paragraphs 50(1)(g), (h) and (i)**

11 Repeal the paragraphs, substitute:

12 (g) the number of arrests made by law enforcement officers of
13 the agency during that year on the basis (wholly or partly) of
14 information 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 (h) the number of instances during that year in which the
23 location and safe recovery of children to whom recovery
24 orders related was assisted (wholly or partly) by information
25 obtained by:

- 26 (i) the use of a surveillance device under a warrant; or
- 27 (ii) access under a warrant to data held in a computer; or
- 28 (iii) an emergency authorisation for the use of a surveillance
29 device; or
- 30 (iv) an emergency authorisation for access to data held in a
31 computer; or
- 32 (v) a tracking device authorisation; and

EXPOSURE DRAFT

Computer access warrants etc. **Schedule 2**
Amendments **Part 1**

- 1 (i) the number of prosecutions for relevant offences that were
2 commenced during that year in which information obtained
3 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;
11 was given in evidence and the number of those prosecutions
12 in which a person was found guilty; and

13 **106 Paragraph 50(1)(j)**

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

15 **107 Subsection 50A(6) (definition of *control order*** 16 ***information*)**

17 Repeal the definition, substitute:

18 ***control order information*** means:

- 19 (a) information that, if made public, could reasonably be
20 expected to enable a reasonable person to conclude that a
21 control order warrant authorising:
22 (i) the use of a surveillance device on particular premises;
23 or
24 (ii) the use of a surveillance device in or on a particular
25 object or class of object; or
26 (iii) the use of a surveillance device in respect of the
27 conversations, activities or location of a particular
28 person;
29 is likely to be, or is not likely to be, in force; or
30 (b) information that, if made public, could reasonably be
31 expected to enable a reasonable person to conclude that a
32 control order access warrant authorising:
33 (i) access to data held in a particular computer; or

EXPOSURE DRAFT

Schedule 2 Computer access warrants etc.

Part 1 Amendments

- 1 (ii) access to data held in a computer on particular premises;
2 or
3 (iii) access to data held in a computer associated with, used
4 by or likely to be used by, a particular person;
5 is likely to be, or is not likely to be, in force.

6 **108 Paragraph 51(b)**

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

8 **109 Paragraphs 52(1)(e), (f), (g) and (h)**

9 Repeal the paragraphs, substitute:

- 10 (e) details of each use by the agency, or by a law enforcement
11 officer of the agency, of information obtained by:
12 (i) the use of a surveillance device by a law enforcement
13 officer of the agency; or
14 (ii) access, by a law enforcement officer of the agency, to
15 data held in a computer;
16 (f) details of each communication by a law enforcement officer
17 of the agency to a person other than a law enforcement
18 officer of the agency of information obtained by:
19 (i) the use of a surveillance device by a law enforcement
20 officer of the agency; or
21 (ii) access, by a law enforcement officer of the agency, to
22 data held in a computer;
23 (g) details of each occasion when, to the knowledge of a law
24 enforcement officer of the agency, information obtained by:
25 (i) the use of a surveillance device by a law enforcement
26 officer of the agency; or
27 (ii) access, by a law enforcement officer of the agency, to
28 data held in a computer;
29 was given in evidence in a relevant proceeding;
30 (h) details of each occasion when, to the knowledge of a law
31 enforcement officer of the agency, information obtained by:
32 (i) the use of a surveillance device by a law enforcement
33 officer of the agency; or
34 (ii) access, by a law enforcement officer of the agency, to
35 data held in a computer;
-

EXPOSURE DRAFT

Computer access warrants etc. **Schedule 2**
Amendments **Part 1**

1 was used in the location and safe recovery of a child to whom
2 a recovery order related;

3 **110 Paragraph 52(1)(j)**

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

5 **111 After subparagraph 53(2)(c)(iic)**

6 Insert:

7 (iiid) if the warrant is a control order access warrant that was
8 issued on the basis of a control order—the date the
9 control order was made; and

10 **112 At the end of subsection 62(1)**

11 Add:

12 ; or (c) anything done by the law enforcement officer in connection
13 with:

14 (i) the communication by a person to another person; or

15 (ii) the making use of; or

16 (iii) the making of a record of; or

17 (iv) the custody of a record of;

18 information obtained from access to data under:

19 (v) a computer access warrant; or

20 (vi) an emergency authorisation for access to data held in a
21 computer.

22 **113 Subsection 62(3)**

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

24 **114 After section 64**

25 Insert:

26 **64A Person with knowledge of a computer or a computer system to** 27 **assist access etc.**

28 (1) A law enforcement officer (or another person on the officer’s
29 behalf) may apply to an eligible Judge or to a nominated AAT
30 member for an order (the *assistance order*) requiring a specified
31

EXPOSURE DRAFT

Schedule 2 Computer access warrants etc.

Part 1 Amendments

- 1 person to provide any information or assistance that is reasonable
2 and necessary to allow the law enforcement officer to do one or
3 more of the following:
- 4 (a) access data held in a computer that is the subject of:
 - 5 (i) a computer access warrant; or
 - 6 (ii) an emergency authorisation given in response to an
7 application under subsection 28(1A), 29(1A) or 30(1A);
 - 8 (b) copy data held in the computer described in paragraph (a) to
9 a data storage device;
 - 10 (c) convert into documentary form or another form intelligible to
11 a law enforcement officer:
 - 12 (i) data held in the computer described in paragraph (a); or
 - 13 (ii) data held in a data storage device to which the data was
14 copied as described in paragraph (b).

15 *Warrants and emergency authorisations relating to relevant*
16 *offences*

- 17 (2) In the case of a computer that is the subject of:
- 18 (a) a computer access warrant issued in relation to a relevant
19 offence; or
 - 20 (b) an emergency authorisation given in response to an
21 application under subsection 28(1A);
- 22 the eligible Judge or nominated AAT member may grant the
23 assistance order if the eligible Judge or nominated AAT member is
24 satisfied that:
- 25 (c) there are reasonable grounds for suspecting that access to
26 data held in the computer is necessary in the course of the
27 investigation for the purpose of enabling evidence to be
28 obtained of:
 - 29 (i) the commission of those offences; or
 - 30 (ii) the identity or location of the offenders; and
 - 31 (d) the specified person is:
 - 32 (i) reasonably suspected of having committed any of the
33 offences to which the warrant or emergency
34 authorisation relates; or
 - 35 (ii) the owner or lessee of the computer or device; or

EXPOSURE DRAFT

Computer access warrants etc. **Schedule 2**
Amendments **Part 1**

- 1 (iii) an employee of the owner or lessee of the computer or
2 device; or
3 (iv) a person engaged under a contract for services by the
4 owner or lessee of the computer or device; or
5 (v) a person who uses or has used the computer or device;
6 or
7 (vi) a person who is or was a system administrator for the
8 system including the computer or device; and
9 (e) the specified person has relevant knowledge of:
10 (i) the computer or device or a computer network of which
11 the computer or device forms or formed a part; or
12 (ii) measures applied to protect data held in the computer or
13 device.

14 *Warrants and emergency authorisations relating to recovery*
15 *orders*

- 16 (3) In the case of a computer that is the subject of:
17 (a) a computer access warrant issued in relation to a recovery
18 order; or
19 (b) an emergency authorisation given in response to an
20 application under subsection 29(1A);
21 the eligible Judge or nominated AAT member may grant the
22 assistance order if the eligible Judge or nominated AAT member is
23 satisfied that:
24 (c) there are reasonable grounds for suspecting that access to
25 data held in the computer may assist in the location and safe
26 recovery of the child to whom the recovery order relates; and
27 (d) the specified person is:
28 (i) the owner or lessee of the computer or
29 (ii) an employee of the owner or lessee of the computer; or
30 (iii) a person engaged under a contract for services by the
31 owner or lessee of the computer; or
32 (iv) a person who uses or has used the computer; or
33 (v) a person who is or was a system administrator for the
34 system including the computer; and
35 (e) the specified person has relevant knowledge of:
-

EXPOSURE DRAFT

Schedule 2 Computer access warrants etc.

Part 1 Amendments

- 1 (i) the computer or a computer network of which the
2 computer forms or formed a part; or
3 (ii) measures applied to protect data held in the computer.

4 *Warrants relating to mutual assistance authorisations*

- 5 (4) In the case of a computer that is the subject of a computer access
6 warrant issued in relation to a mutual assistance authorisation, the
7 eligible Judge or nominated AAT member may grant the assistance
8 order if the eligible Judge or nominated AAT member is satisfied
9 that:
- 10 (a) there are reasonable grounds for suspecting that access to
11 data held in the computer is necessary, in the course of the
12 investigation or investigative proceeding to which the
13 authorisation relates, for the purpose of enabling evidence to
14 be obtained of:
- 15 (i) the commission of the offence to which the
16 authorisation relates; or
17 (ii) the identity or location of the persons suspected of
18 committing the offence; and
- 19 (b) the specified person is:
- 20 (i) reasonably suspected of committing the offence to
21 which the authorisation relates; or
22 (ii) the owner or lessee of the computer; or
23 (iii) an employee of the owner or lessee of the computer; or
24 (iv) a person engaged under a contract for services by the
25 owner or lessee of the computer; or
26 (v) a person who uses or has used the computer; or
27 (vi) a person who is or was a system administrator for the
28 system including the computer; and
- 29 (c) the specified person has relevant knowledge of:
- 30 (i) the computer or a computer network of which the
31 computer forms or formed a part; or
32 (ii) measures applied to protect data held in the computer.

EXPOSURE DRAFT

Computer access warrants etc. **Schedule 2**
Amendments **Part 1**

1

Warrants relating to integrity operations

2

(5) In the case of a computer that is the subject of a computer access warrant issued in relation to an integrity operation, the eligible Judge or nominated AAT member may grant the assistance order if the eligible Judge or nominated AAT member is satisfied that:

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

- (a) there are reasonable grounds for suspecting that access to data held in the computer will assist the conduct of the integrity operation by enabling evidence to be obtained relating to the integrity, location or identity of a particular staff member of the target agency; and
- (b) the specified person is:
 - (i) the staff member; or
 - (ii) the owner or lessee of the computer; or
 - (iii) an employee of the owner or lessee of the computer; or
 - (iv) a person engaged under a contract for services by the owner or lessee of the computer; or
 - (v) a person who uses or has used the computer; or
 - (vi) a person who is or was a system administrator for the system including the computer; and
- (c) the specified person has relevant knowledge of:
 - (i) the computer or a computer network of which the computer forms or formed a part; or
 - (ii) measures applied to protect data held in the computer.

24

Warrants relating to control orders

25

26

27

28

29

30

31

32

33

34

(6) In the case of a computer that is subject to a computer access warrant issued on the basis of a control order, the eligible Judge or nominated AAT member may grant the assistance order if the eligible Judge or nominated AAT member is satisfied that:

- (a) there are reasonable grounds for suspecting that access to the data held in the computer would be likely to substantially assist in:
 - (i) protecting the public from a terrorist act; or
 - (ii) preventing the provision of support for, or the facilitation of, a terrorist act; or

EXPOSURE DRAFT

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 (b) the specified person is:
8 (i) the subject of the control order; or
9 (ii) the owner or lessee of the computer; or
10 (iii) an employee of the owner or lessee of the computer; or
11 (iv) a person engaged under a contract for services by the
12 owner or lessee of the computer; or
13 (v) a person who uses or has used the computer; or
14 (vi) a person who is or was a system administrator for the
15 system including the computer; and
16 (c) the specified person has relevant knowledge of:
17 (i) the computer or a computer network of which the
18 computer forms or formed a part; or
19 (ii) measures applied to protect data held in the computer.

20 *Emergency authorisations relating to risk of loss of evidence*

- 21 (7) In the case of a computer that is the subject of an emergency
22 authorisation given in response to an application under
23 subsection 30(1A), the eligible Judge or nominated AAT member
24 may grant the assistance order if the eligible Judge or nominated
25 AAT member is satisfied that:
26 (a) there are reasonable grounds for suspecting that access to
27 data held in the computer is necessary to prevent the loss of
28 any evidence relevant to the investigation to which the
29 subsection 30(1A) application relates; and
30 (b) the specified person is:
31 (i) reasonably suspected of having committed any of the
32 offences to which the emergency authorisation relates;
33 or
34 (ii) the owner or lessee of the computer or device; or

EXPOSURE DRAFT

Computer access warrants etc. **Schedule 2**
Amendments **Part 1**

- 1 (iii) an employee of the owner or lessee of the computer or
2 device; or
3 (iv) a person engaged under a contract for services by the
4 owner or lessee of the computer or device; or
5 (v) a person who uses or has used the computer or device;
6 or
7 (vi) a person who is or was a system administrator for the
8 system including the computer or device; and
9 (c) the specified person has relevant knowledge of:
10 (i) the computer or device or a computer network of which
11 the computer or device forms or formed a part; or
12 (ii) measures applied to protect data held in the computer or
13 device.

14 *Offence*

- 15 (8) A person commits an offence if:
16 (a) the person is subject to an order under this section; and
17 (b) the person is capable of complying with a requirement in the
18 order; and
19 (c) the person omits to do an act; and
20 (d) the omission contravenes the requirement.

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

23 **115 After subsection 65(1)**

24 Insert:

- 25 (1A) If:
26 (a) information or a record is purportedly obtained through
27 accessing, under a computer access warrant or emergency
28 authorisation, particular data held in a computer; and
29 (b) there is a defect or irregularity in relation to the warrant or
30 emergency authorisation; and
31 (c) but for that defect or irregularity, the warrant or emergency
32 authorisation would be a sufficient authority for accessing the
33 data;

EXPOSURE DRAFT

Schedule 2 Computer access warrants etc.

Part 1 Amendments

1 then:
2 (d) access to the data is taken to be as valid; and
3 (e) the information or record obtained through accessing the data
4 may be dealt with, or given in evidence in any proceeding;
5 as if the warrant or emergency authorisation did not have that
6 defect or irregularity.

7 **116 Subsection 65(2)**

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

9 **117 After subsection 65A(2)**

10 Insert:

11 *Control order access warrant*

12 (2A) If:

- 13 (a) a control order access warrant was issued on the basis that an
14 interim control order was in force; and
15 (b) a court subsequently declares the interim control order to be
16 void;

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

- 19 (c) in the purported execution of the warrant; or
20 (d) in the purported exercise of a power, or the purported
21 performance of a function or duty, in a case where the
22 purported exercise of the power, or the purported
23 performance of the function or duty, is consequential on the
24 warrant.

25 (2B) Subsection (2A) does not apply to a thing done, or omitted to be
26 done, at a particular time if, at that time, the person knew, or ought
27 reasonably to have known, of the declaration.

28 **118 Section 65B (heading)**

29 Repeal the heading, substitute:

EXPOSURE DRAFT

Computer access warrants etc. **Schedule 2**
Amendments **Part 1**

1 **65B Dealing with information obtained under a control order**
2 **warrant, control order access warrant, tracking device**
3 **authorisation etc.—control order declared to be void**

4 **119 After subparagraph 65B(1)(a)(i)**

5 Insert:

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

8 ***Telecommunications Act 1997***

9 **119A After paragraph 313(7)(c)**

10 Insert:

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

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

14 **120 Subsection 5(1)**

15 Insert:

16 ***ASIO computer access intercept information*** means information
17 obtained under:

- 18 (a) an ASIO computer access warrant; or
19 (b) subsection 25A(8) of the *Australian Security Intelligence*
20 *Organisation Act 1979*; or
21 (c) subsection 27A(3C) of the *Australian Security Intelligence*
22 *Organisation Act 1979*; or
23 (d) an authorisation under section 27E of the *Australian Security*
24 *Intelligence Organisation Act 1979*; or
25 (e) subsection 27E(6) of the *Australian Security Intelligence*
26 *Organisation Act 1979*;

27 by intercepting a communication passing over a
28 telecommunications system.

29 ***ASIO computer access warrant*** means:

EXPOSURE DRAFT

Schedule 2 Computer access warrants etc.

Part 1 Amendments

- 1 (a) a warrant issued under section 25A of the *Australian Security*
2 *Intelligence Organisation Act 1979*; or
3 (b) a warrant issued under section 27A of the *Australian Security*
4 *Intelligence Organisation Act 1979* that authorises the
5 Organisation to do any of the acts or things referred to in
6 subsection 25A(4) or (8) of that Act; or
7 (c) an authorisation under section 27E of the *Australian Security*
8 *Intelligence Organisation Act 1979*.

9 ***general computer access intercept information*** means information
10 obtained under a general computer access warrant by intercepting a
11 communication passing over a telecommunications system.

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

14 **121 Subsection 5(1) (at the end of the definition of *restricted***
15 ***record*)**

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

18 **122 Subsection 5(1) (paragraph (b) of the definition of**
19 ***warrant*)**

20 After “definition”, insert “, a general computer access warrant or an
21 ASIO computer access warrant”.

22 **123 After paragraph 7(2)(b)**

23 Insert:

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

29 **123A Subsection 31(1)**

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

EXPOSURE DRAFT

Computer access warrants etc. **Schedule 2**
Amendments **Part 1**

- 1 system:
2 (a) if one or more carriers are specified in the request for the
3 purposes of this paragraph—by:
4 (i) employees of the security authority authorised under
5 section 31B; and
6 (ii) employees of those carriers; or
7 (b) if no carriers are specified in the request for the purposes of
8 paragraph (a)—by employees of the security authority
9 authorised under section 31B.

10 **123B Subsection 31A(1)**

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

- 13 system:
14 (a) if one or more carriers are specified in the request for the
15 purposes of paragraph 31(1)(a)—by:
16 (i) employees of the security authority authorised under
17 section 31B; and
18 (ii) employees of those carriers; or
19 (b) if no carriers are specified in the request for the purposes of
20 paragraph 31(1)(a)—by employees of the security authority
21 authorised under section 31B.

22 **123BA After subsection 31A(4)**

23 Insert:

- 24 (4A) If paragraph (1)(a) applies to the authorisation, this Part does not
25 require that an authorised interception must involve:
26 (a) one or more employees of the security authority referred to in
27 that paragraph; and
28 (b) one or more employees of a carrier referred to in that
29 paragraph;
30 acting together or in the presence of each other.

31 **123C After section 31A**

32 Insert:

EXPOSURE DRAFT

Schedule 2 Computer access warrants etc.

Part 1 Amendments

1 **31AA Carrier to be notified of authorisation etc.**

2 (1) If:

- 3 (a) the Attorney-General gives a section 31A authorisation in
4 response to an application made by:
5 (i) the head (however described) of a security authority; or
6 (ii) a person acting as that head; and
7 (b) the authorisation covers the employees of a carrier;
8 the head (however described) of the security authority, or a person
9 acting as that head, must cause a copy of the authorisation to be
10 given to the authorised representative of the carrier as soon as
11 practicable.

12 (2) If:

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

25 **123D At the end of Part 2-4**

26 Add:

27 **31E Employees of security authorities**

28 (1) For the purposes of this Part:

- 29 (a) an ASIO employee is taken to be an employee of the
30 Organisation; and
31 (b) an ASIO affiliate is taken to be an employee of the
32 Organisation.

EXPOSURE DRAFT

Computer access warrants etc. **Schedule 2**
Amendments **Part 1**

- 1 (2) For the purposes of this Part, if:
2 (a) a person is a staff member (within the meaning of the
3 *Intelligence Services Act 2001*) of an agency (within the
4 meaning of that Act); and
5 (b) the agency is a security authority;
6 the person is taken to be an employee of the security authority.

7 **124 After section 63AA**

8 Insert:

9 **63AB Dealing in general computer access intercept information**

- 10 (1) A person may, for the purposes of doing a thing authorised by a
11 general computer access warrant:
12 (a) communicate general computer access intercept information
13 to another person; or
14 (b) make use of general computer access intercept information;
15 or
16 (c) make a record of general computer access intercept
17 information; or
18 (d) give general computer access intercept information in
19 evidence in a proceeding.
- 20 (2) A person may:
21 (a) communicate general computer access intercept information
22 to another person; or
23 (b) make use of general computer access intercept information;
24 or
25 (c) make a record of general computer access intercept
26 information;
27 if the information relates, or appears to relate, to the involvement,
28 or likely involvement, of a person in one or more of the following
29 activities:
30 (d) activities that present a significant risk to a person's safety;
31 (e) acting for, or on behalf of, a foreign power (within the
32 meaning of the *Australian Security Intelligence Organisation*
33 *Act 1979*);

EXPOSURE DRAFT

Schedule 2 Computer access warrants etc.

Part 1 Amendments

- 1 (f) activities that are, or are likely to be, a threat to security;
2 (g) activities that pose a risk, or are likely to pose a risk, to the
3 operational security (within the meaning of the *Intelligence*
4 *Services Act 2001*) of the Organisation or of ASIS, AGO or
5 ASD (within the meanings of that Act);
6 (h) activities related to the proliferation of weapons of mass
7 destruction or the movement of goods listed from time to
8 time in the Defence and Strategic Goods List (within the
9 meaning of regulation 13E of the *Customs (Prohibited*
10 *Exports) Regulations 1958*);
11 (i) activities related to a contravention, or an alleged
12 contravention, by a person of a UN sanction enforcement law
13 (within the meaning of the *Charter of the United Nations Act*
14 *1945*).

15 **63AC Dealing in ASIO computer access intercept information**

- 16 (1) A person may, for the purposes of doing a thing authorised by an
17 ASIO computer access warrant:
18 (a) communicate ASIO computer access intercept information to
19 another person; or
20 (b) make use of ASIO computer access intercept information; or
21 (c) make a record of ASIO computer access intercept
22 information; or
23 (d) give ASIO computer access intercept information in evidence
24 in a proceeding.
- 25 (2) A person may:
26 (a) communicate ASIO computer access intercept information to
27 another person; or
28 (b) make use of ASIO computer access intercept information; or
29 (c) make a record of ASIO computer access intercept
30 information;
31 if the information relates, or appears to relate, to the involvement,
32 or likely involvement, of a person in one or more of the following
33 activities:
34 (d) activities that present a significant risk to a person's safety;

EXPOSURE DRAFT

Computer access warrants etc. **Schedule 2**
Amendments **Part 1**

- 1 (e) acting for, or on behalf of, a foreign power (within the
2 meaning of the *Australian Security Intelligence Organisation*
3 *Act 1979*);
4 (f) activities that are, or are likely to be, a threat to security;
5 (g) activities that pose a risk, or are likely to pose a risk, to the
6 operational security (within the meaning of the *Intelligence*
7 *Services Act 2001*) of the Organisation or of ASIS, AGO or
8 ASD (within the meanings of that Act);
9 (h) activities related to the proliferation of weapons of mass
10 destruction or the movement of goods listed from time to
11 time in the Defence and Strategic Goods List (within the
12 meaning of regulation 13E of the *Customs (Prohibited*
13 *Exports) Regulations 1958*);
14 (i) activities related to a contravention, or an alleged
15 contravention, by a person of a UN sanction enforcement law
16 (within the meaning of the *Charter of the United Nations Act*
17 *1945*).

18 **124A At the end of section 63B**

19 Add:

- 20 (5) If an employee of a carrier has obtained lawfully intercepted
21 information under a section 31A authorisation that was given in
22 response to an application made by the head (however described)
23 of a security authority or a person acting as that head, the employee
24 may:
25 (a) communicate the information to:
26 (i) an employee of the security authority; or
27 (ii) another employee of the carrier; or
28 (iii) if the authorisation covers the employees of one or more
29 other carriers—an employee of any of those other
30 carriers; or
31 (b) make use of the information; or
32 (c) make a record of the information;
33 if:
34 (d) the employee does so for the purposes of the development or
35 testing of technologies, or interception capabilities, to which
36 the authorisation relates; and

EXPOSURE DRAFT

Schedule 2 Computer access warrants etc.

Part 1 Amendments

- 1 (e) the communication or use of the information, or the making
2 of the record, as the case may be, does not contravene a
3 condition to which the authorisation is subject.

4 **125 Paragraph 64(1)(a)**

5 After “foreign intelligence information”, insert “or ASIO computer
6 access intercept information”.

7 **126 Paragraph 65(1)(a)**

8 After “information”, insert “other than ASIO computer access intercept
9 information”.

10 **126AA At the end of section 65 (after the note)**

11 Add:

12 (4) If lawfully intercepted information was obtained under a
13 section 31A authorisation, subsection (1) of this section does not
14 authorise the communication of the information in accordance with
15 subsection 18(3) of the *Australian Security Intelligence*
16 *Organisation Act 1979* to:

- 17 (a) a staff member of an authority of the Commonwealth; or
18 (b) a staff member of an authority of a State;

19 unless the communication is for the purpose of the development or
20 testing of technologies, or interception capabilities, of:

- 21 (c) that authority; or
22 (d) the Organisation.

23 (5) If lawfully intercepted information was obtained under a
24 section 31A authorisation, subsection (1) of this section does not
25 authorise the communication of the information in accordance with
26 subsection 18(4A) of the *Australian Security Intelligence*
27 *Organisation Act 1979* to a staff member of ASIS, ASD or AGO
28 unless the communication is for the purpose of the development or
29 testing of technologies, or interception capabilities, of:

- 30 (a) ASIS, ASD or AGO, as the case requires; or
31 (b) the Organisation.

EXPOSURE DRAFT

Computer access warrants etc. **Schedule 2**
Amendments **Part 1**

1 (6) If lawfully intercepted information was obtained under a
2 section 31A authorisation, subsection (1) of this section does not
3 authorise the communication of the information in accordance with
4 subsection 19A(4) of the *Australian Security Intelligence*
5 *Organisation Act 1979* to a staff member of a body referred to in
6 paragraph 19A(1)(d) or (e) of that Act unless the communication is
7 for the purpose of the development or testing of technologies, or
8 interception capabilities, of:
9 (a) that body; or
10 (b) the Organisation.

11 (7) For the purposes of subsections (4), (5) and (6), *authority of the*
12 *Commonwealth, authority of a State, ASIS, ASD, AGO* and *staff*
13 *member* have the same respective meanings as in the *Australian*
14 *Security Intelligence Organisation Act 1979*.

15 **126A Paragraph 65A(1)(a)**

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

18 **127 Paragraph 67(1)(a)**

19 After “foreign intelligence information”, insert “or general computer
20 access intercept information”.

21 **128 Section 68**

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

24 **129 Subsection 74(1)**

25 After “foreign intelligence information”, insert “, general computer
26 access intercept information or ASIO computer access intercept
27 information”.

28 **130 Subsection 75(1)**

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

30 **131 Paragraphs 77(1)(a) and (b)**

31 After “63A,”, insert “63AB, 63AC,”.

EXPOSURE DRAFT

Schedule 2 Computer access warrants etc.

Part 1 Amendments

1 **131A After paragraph 108(2)(ca)**

2 Insert:

3 (cb) accessing a stored communication under a general computer
4 access warrant; or

EXPOSURE DRAFT

Computer access warrants etc. **Schedule 2**
Application provisions **Part 2**

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.

EXPOSURE DRAFT

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 **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

EXPOSURE DRAFT

Computer access warrants etc. **Schedule 2**
Amendments contingent on the commencement of the Crimes Legislation Amendment
(International Crime Cooperation and Other Measures) Act 2018 **Part 3**

- 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*.

International War Crimes Tribunals Act 1995

134 After Division 1A of Part 4

20 Insert:

Division 1B—Requests for access to data held in computers

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

EXPOSURE DRAFT

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.
-

EXPOSURE DRAFT

Computer access warrants etc. **Schedule 2**
Amendments contingent on the commencement of the Crimes Legislation Amendment
(International Crime Cooperation and Other Measures) Act 2018 **Part 3**

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

EXPOSURE DRAFT

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 **140 Subparagraph 27D(1)(b)(iv)**

2 Repeal the paragraph, substitute:

- 3 (iv) if the warrant relates to an international assistance
4 authorisation—each offence to which the authorisation
5 relates; and

6 **141 Paragraph 27E(3)(c)**

7 Omit “a mutual assistance authorisation”, substitute “an international
8 assistance authorisation”.

9 **142 Paragraph 27H(4)(a)**

10 Omit “a mutual assistance authorisation”, substitute “an international
11 assistance authorisation”.

12 **143 Subparagraph 27H(4)(b)(i)**

13 Repeal the subparagraph, substitute:

- 14 (i) the commission of any offence to which the
15 authorisation relates; or

16 **144 Paragraph 27H(9)(c)**

17 Repeal the paragraph, substitute:

- 18 (c) if the warrant was issued in relation to an international
19 assistance authorisation—of enabling evidence to be obtained
20 of:
21 (i) the commission of any offence to which the
22 authorisation relates; or
23 (ii) the identity or location of the persons suspected of
24 committing the offence;

25 **145 Subsection 64A(4)**

26 Repeal the subsection, substitute:

27 *Warrants relating to international assistance authorisations*

- 28 (4) In the case of a computer that is the subject of a computer access
29 warrant issued in relation to an international assistance
30 authorisation, the eligible Judge or nominated AAT member may
-

EXPOSURE DRAFT

Computer access warrants etc. **Schedule 2**
Amendments contingent on the commencement of the Crimes Legislation Amendment
(International Crime Cooperation and Other Measures) Act 2018 **Part 3**

- 1 grant the assistance order if the eligible Judge or nominated AAT
2 member is satisfied that:
- 3 (a) there are reasonable grounds for suspecting that access to
4 data held in the computer is necessary, in the course of the
5 investigation or investigative proceeding to which the
6 authorisation relates, for the purpose of enabling evidence to
7 be obtained of:
- 8 (i) the commission of an offence to which the authorisation
9 relates; or
- 10 (ii) the identity or location of the persons suspected of
11 committing the offence; and
- 12 (b) the specified person is:
- 13 (i) reasonably suspected of committing an offence to which
14 the authorisation relates; or
- 15 (ii) the owner or lessee of the computer; or
- 16 (iii) an employee of the owner or lessee of the computer; or
- 17 (iv) a person engaged under a contract for services by the
18 owner or lessee of the computer; or
- 19 (v) a person who uses or has used the computer; or
- 20 (vi) a person who is or was a system administrator for the
21 system including the computer; and
- 22 (c) 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 **146 Application of amendments**

27 The amendments made by this Part apply in relation to a request made
28 to the Attorney-General by the ICC, a Tribunal or a foreign country:

- 29 (a) at or after the commencement of this item; or
- 30 (b) before the commencement of this item, if, immediately
31 before that commencement, the Attorney-General had yet to
32 make a decision on the request;

33 whether conduct, a crime or an offence to which the request relates
34 occurred before, on or after that commencement.

EXPOSURE DRAFT

Schedule 3 Search warrants issued under the Crimes Act 1914

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

EXPOSURE DRAFT

Search warrants issued under the Crimes Act 1914 **Schedule 3**

1 (c) the person can (with the use of appropriate equipment) access
2 particular data provided by the service;
3 the data is **account-based data** in relation to the person.

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

5 (a) an electronic service has accounts for end-users; and

6 (b) either:

7 (i) a deceased person held, before the person's death, an
8 account with the electronic service; or

9 (ii) a deceased person, before the person's death, was, or
10 was likely to be, a user of an account with the electronic
11 service; and

12 (c) the deceased person could, before the person's death (with
13 the use of appropriate equipment), access particular data
14 provided by the service;

15 the data is **account-based data** in relation to the deceased person.

16 (3) For the purposes of this section, **account** has the same meaning as
17 in the *Enhancing Online Safety Act 2015*.

18 **3 After subsection 3F(2)**

19 Insert:

20 (2A) A warrant that is in force authorises the executing officer or a
21 constable assisting:

22 (a) to use:

23 (i) a computer, or data storage device, found in the course
24 of a search authorised under the warrant; or

25 (ii) a telecommunications facility operated or provided by
26 the Commonwealth or a carrier; or

27 (iii) any other electronic equipment; or

28 (iv) a data storage device;

29 for the purpose of obtaining access to data (the **relevant data**)
30 that is held in the computer or device mentioned in
31 subparagraph (i) at any time when the warrant is in force, in
32 order to determine whether the relevant data is evidential
33 material of a kind specified in the warrant; and

EXPOSURE DRAFT

Schedule 3 Search warrants issued under the Crimes Act 1914

- 1 (b) if necessary to achieve the purpose mentioned in
2 paragraph (a)—to add, copy, delete or alter other data in the
3 computer or device mentioned in subparagraph (a)(i); and
4 (c) if, having regard to other methods (if any) of obtaining access
5 to the relevant data which are likely to be as effective, it is
6 reasonable in all the circumstances to do so:
7 (i) to use any other computer or a communication in transit
8 to access the relevant data; and
9 (ii) if necessary to achieve that purpose—to add, copy,
10 delete or alter other data in the computer or the
11 communication in transit; and
12 (d) to copy any data to which access has been obtained, and that:
13 (i) appears to be relevant for the purposes of determining
14 whether the relevant data is evidential material of a kind
15 specified in the warrant; or
16 (ii) is evidential material of a kind specified in the warrant;
17 and
18 (e) to do any other thing reasonably incidental to any of the
19 above.

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

- 25 (2B) A warrant that is in force authorises the executing officer or a
26 constable assisting:
27 (a) to use:
28 (i) a computer found in the course of a search authorised
29 under the warrant; or
30 (ii) a telecommunications facility operated or provided by
31 the Commonwealth or a carrier; or
32 (iii) any other electronic equipment;
33 for the purpose of obtaining access to data (the ***relevant***
34 ***account-based data***) that is account-based data in relation to:
35 (iv) a person who is the owner or lessee of the computer
36 mentioned in subparagraph (i); or

EXPOSURE DRAFT

Search warrants issued under the Crimes Act 1914 **Schedule 3**

- 1 (v) a person who uses or has used the computer mentioned
2 in subparagraph (i); or
3 (vi) a deceased person who, before the person's death, was
4 the owner or lessee of the computer mentioned in
5 subparagraph (i); or
6 (vii) a deceased person who, before the person's death, used
7 the computer mentioned in subparagraph (i);
8 in order to determine whether the relevant account-based data
9 is evidential material of a kind specified in the warrant; and
10 (b) if necessary to achieve the purpose mentioned in
11 paragraph (a)—to add, copy, delete or alter other data in the
12 computer mentioned in subparagraph (a)(i); and
13 (c) if, having regard to other methods (if any) of obtaining access
14 to the relevant account-based data which are likely to be as
15 effective, it is reasonable in all the circumstances to do so:
16 (i) to use any other computer or a communication in transit
17 to access the relevant account-based data; and
18 (ii) if necessary to achieve that purpose—to add, copy,
19 delete or alter other data in the computer or the
20 communication in transit; and
21 (d) to copy any data to which access has been obtained, and that:
22 (i) appears to be relevant for the purposes of determining
23 whether the relevant account-based data is evidential
24 material of a kind specified in the warrant; or
25 (ii) is evidential material of a kind specified in the warrant;
26 and
27 (e) to do any other thing reasonably incidental to any of the
28 above.
- 29 (2C) Subsections (2A) and (2B) do not authorise the addition, deletion
30 or alteration of data, or the doing of any thing, that is likely to:
31 (a) materially interfere with, interrupt or obstruct:
32 (i) a communication in transit; or
33 (ii) the lawful use by other persons of a computer;
34 unless the addition, deletion or alteration, or the doing of the
35 thing, is necessary to do one or more of the things specified
36 in the warrant; or
-

EXPOSURE DRAFT

Schedule 3 Search warrants issued under the Crimes Act 1914

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

3 (2D) In the case of a warrant that is in force in relation to premises, it is
4 immaterial whether a thing mentioned in subsection (2A) or (2B) is
5 done:

6 (a) at the premises; or

7 (b) at any other place.

8 (2E) In the case of a warrant that is in force in relation to a person, it is
9 immaterial whether a thing mentioned in subsection (2A) or (2B) is
10 done:

11 (a) in the presence of the person; or

12 (b) at any other place.

13 **4 Subsection 3K(3A)**

14 Omit “14 days.”, substitute:

15 whichever of the following is applicable:

16 (a) if the thing is a computer or data storage device—30 days;

17 (b) otherwise—14 days.

18 **5 Subsection 3K(3B)**

19 Omit “14 days”, substitute “the time applicable under subsection (3A)”.

20 **6 Subsection 3K(3D)**

21 Omit “7 days.”, substitute:

22 whichever of the following is applicable:

23 (a) if the thing is a computer or data storage device—14 days;

24 (b) otherwise—7 days.

25 **6A At the end of section 3K**

26 Add:

27 *Extended powers of examination and processing*

28 (5) For the purposes of this section, if a computer or data storage
29 device (the *relevant computer or device*) was found in the course

EXPOSURE DRAFT

Search warrants issued under the Crimes Act 1914 **Schedule 3**

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

of a search authorised under a warrant, the examination or processing of the relevant computer or device may include:

(a) using:

- (i) the relevant computer or device; or
- (ii) a telecommunications facility operated or provided by the Commonwealth or a carrier; or
- (iii) any other electronic equipment; or
- (iv) a data storage device;

for the purpose of obtaining access to data (the *relevant data*) that is held in the relevant computer or device in order to determine whether the relevant computer or device is a thing that may be seized under the warrant; and

(b) if necessary to achieve the purpose mentioned in paragraph (a)—to add, copy, delete or alter other data in the relevant computer or device; and

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

- (i) to use any other computer or a communication in transit to access the relevant data; and
- (ii) if necessary to achieve that purpose—to add, copy, delete or alter other data in the computer or the communication in transit; and

(d) to copy any data to which access has been obtained, and that appears to be relevant for the purposes of determining whether the relevant computer or device is a thing that may be seized under the warrant; and

(e) to do any other thing reasonably incidental to any of the above.

(6) For the purposes of this section, if a computer (the *relevant computer*) was found in the course of a search authorised under a warrant, the examination or processing of the relevant computer may include:

(a) using:

- (i) the relevant computer; or

EXPOSURE DRAFT

Schedule 3 Search warrants issued under the Crimes Act 1914

- 1 (ii) a telecommunications facility operated or provided by
2 the Commonwealth or a carrier; or
3 (iii) any other electronic equipment;
4 for the purpose of obtaining access to data (the *relevant*
5 *account-based data*) that is account-based data in relation to:
6 (iv) a person who is the owner or lessee of the relevant
7 computer; or
8 (v) a person who uses or has used the relevant computer; or
9 (vi) a deceased person who, before the person's death, was
10 the owner or lessee of the relevant computer; or
11 (vii) a deceased person who, before the person's death, used
12 the relevant computer;
13 in order to determine whether the relevant computer is a
14 thing that may be seized under the warrant; and
15 (b) if necessary to achieve the purpose mentioned in
16 paragraph (a)—to add, copy, delete or alter other data in the
17 relevant computer; and
18 (c) if, having regard to other methods (if any) of obtaining access
19 to the relevant account-based data which are likely to be as
20 effective, it is reasonable in all the circumstances to do so:
21 (i) to use any other computer or a communication in transit
22 to access the relevant account-based data; and
23 (ii) if necessary to achieve that purpose—to add, copy,
24 delete or alter other data in the computer or the
25 communication in transit; and
26 (d) to copy any data to which access has been obtained, and that
27 appears to be relevant for the purposes of determining
28 whether the relevant computer is a thing that may be seized
29 under the warrant; and
30 (e) to do any other thing reasonably incidental to any of the
31 above.
- 32 (7) Subsections (5) and (6) do 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
36 (ii) the lawful use by other persons of a computer;
-

EXPOSURE DRAFT

Search warrants issued under the Crimes Act 1914 **Schedule 3**

- 1 unless the addition, deletion or alteration, or the doing of the
2 thing, is necessary to determine:
- 3 (iii) in the case of subsection (5)—whether the relevant
4 computer or device is a thing that may be seized under
5 the warrant referred to in that subsection; or
- 6 (iv) in the case of subsection (6)—whether the relevant
7 computer is a thing that may be seized under the warrant
8 referred to in that subsection; or
- 9 (b) cause any other material loss or damage to other persons
10 lawfully using a computer.
- 11 (8) In the case of a warrant that was in force in relation to premises, it
12 is immaterial whether a thing mentioned in subsection (5) or (6) is
13 done:
- 14 (a) at the premises; or
15 (b) at any other place.
- 16 (9) In the case of a warrant that was in force in relation to a person, it
17 is immaterial whether a thing mentioned in subsection (5) or (6) is
18 done:
- 19 (a) in the presence of the person; or
20 (b) at any other place.

21 **7 Subsection 3LAA(1)**

- 22 Omit “to access data (including data held at another place).”, substitute:
23 to:
24 (a) access data (including data held at another place); or
25 (b) access account-based data.

26 **8 After subparagraph 3LA(1)(a)(i)**

- 27 Insert:
28 (ia) is found in the course of an ordinary search of a person,
29 or a frisk search of a person, authorised by a warrant
30 under section 3E; or

31 **9 Subsection 3LA(5)**

- 32 Repeal the subsection, substitute:
-

EXPOSURE DRAFT

Schedule 3 Search warrants issued under the Crimes Act 1914

1

Offences

2

(5) 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 order; and

5

6

(c) the person omits to do an act; and

7

(d) the omission contravenes the requirement.

8

Penalty: Imprisonment for 5 years or 300 penalty units, or both.

9

(6) A person commits an offence if:

10

(a) the person is subject to an order under this section; and

11

(b) the person is capable of complying with a requirement in the order; and

12

13

(c) the person omits to do an act; and

14

(d) the omission contravenes the requirement; and

15

(e) the offence to which the relevant warrant relates is:

16

(i) a serious offence; or

17

(ii) a serious terrorism offence.

18

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

19

20

10 After paragraph 3N(2)(a)

21

Insert:

22

(aa) the thing embodies data that was accessed under the warrant at a place other than the premises; or

23

24

11 After subsection 3ZQV(3)

25

Insert:

26

(3A) If the electronic equipment was seized under a warrant,

27

subsection (2) does not apply to data that was generated after the expiry of the warrant.

28

EXPOSURE DRAFT

Search warrants issued under the Crimes Act 1914 **Schedule 3**

1 **12 Application of amendments**

2 The amendments of sections 3F, 3K, 3LAA, 3LA, 3N and 3ZQV of the
3 *Crimes Act 1914* made by this Schedule apply in relation to a warrant
4 issued after the commencement of this item.

EXPOSURE DRAFT

EXPOSURE DRAFT

Schedule 4 Search warrants issued under the Customs Act 1901

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:

EXPOSURE DRAFT

Search warrants issued under the Customs Act 1901 **Schedule 4**

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

EXPOSURE DRAFT

Schedule 4 Search warrants issued under the Customs Act 1901

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,

EXPOSURE DRAFT

Search warrants issued under the Customs Act 1901 **Schedule 4**

- 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.
-

EXPOSURE DRAFT

Schedule 4 Search warrants issued under the Customs Act 1901

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

EXPOSURE DRAFT

Search warrants issued under the Customs Act 1901 **Schedule 4**

- 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.

EXPOSURE DRAFT

Schedule 4 Search warrants issued under the Customs Act 1901

- 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:

EXPOSURE DRAFT

Schedule 4 Search warrants issued under the Customs Act 1901

- 1 operating the electronic equipment to a disk, tape or other
2 associated device.
- 3 (3) If the Comptroller-General of Customs is satisfied that the data is
4 not required (or is no longer required) for:
- 5 (a) investigating an offence against a law of the Commonwealth,
6 a State or a Territory; or
- 7 (b) judicial proceedings or administrative review proceedings; or
8 (c) investigating or resolving a complaint under the *Ombudsman*
9 *Act 1976* or the *Privacy Act 1988*;
- 10 the Comptroller-General of Customs must arrange for:
- 11 (d) the removal of the data from any device subject to customs
12 control; and
- 13 (e) the destruction of any other reproduction of the data subject
14 to customs control.
- 15 (4) If the executing officer or a person assisting, after operating the
16 equipment, finds that evidential material is accessible by doing so,
17 the executing officer or person assisting may:
- 18 (a) seize the equipment and any disk, tape or other associated
19 device; or
- 20 (b) if the material can be put in documentary form—put the
21 material in that form and seize the documents so produced.
- 22 (5) The executing officer or a person assisting may seize equipment
23 under paragraph (4)(a) only if:
- 24 (a) it is not practicable to copy the data as mentioned in
25 subsection (2) or to put the material in documentary form as
26 mentioned in paragraph (4)(b); or
- 27 (b) possession of the equipment by the person referred to in
28 paragraph 200(2)(b) or (c) (as the case requires) could
29 constitute an offence.

9 Paragraphs 201A(1)(a), (b) and (c)

30 Repeal the paragraphs, substitute:

- 31 (a) access data held in, or accessible from, a computer or data
32 storage device that:
- 33 (i) is on warrant premises; or
- 34

EXPOSURE DRAFT

Search warrants issued under the Customs Act 1901 **Schedule 4**

- 1 (ii) has been seized under this Subdivision; or
2 (iii) is found in the course of an ordinary search of a person,
3 or a frisk search of a person, authorised by a search
4 warrant;
5 (b) copy data held in, or accessible from, a computer, or data
6 storage device, described in paragraph (a) to another data
7 storage device;
8 (c) convert into documentary form or another form intelligible to
9 an executing officer:
10 (i) data held in, or accessible from, a computer, or data
11 storage device, described in paragraph (a); or
12 (ii) data held in a data storage device to which the data was
13 copied as described in paragraph (b).

14 **10 Paragraph 201A(2)(a)**

15 After “the computer”, insert “or data storage device”.

16 **11 Subparagraph 201A(2)(b)(ii)**

17 After “the computer”, insert “or device”.

18 **12 Subparagraph 201A(2)(b)(iii)**

19 Omit “; and”, substitute “or device; or”.

20 **13 At the end of paragraph 201A(2)(b)**

21 Add:

- 22 (iv) a person engaged under a contract for services by the
23 owner or lessee of the computer or device; or
24 (v) a person who uses or has used the computer or device;
25 or
26 (vi) a person who is or was a system administrator for the
27 system including the computer or device; and

28 **14 Subparagraph 201A(2)(c)(i)**

29 After “the computer or”, insert “device or”.

30 **15 Subparagraph 201A(2)(c)(i)**

31 After “which the computer”, insert “or device”.

EXPOSURE DRAFT

Schedule 4 Search warrants issued under the Customs Act 1901

1 **16 Subparagraph 201A(2)(c)(i)**

2 After “forms”, insert “or formed”.

3 **17 Subparagraph 201A(2)(c)(ii)**

4 After “the computer”, insert “or device”.

5 **18 Subsection 201A(3)**

6 Repeal the subsection, substitute:

7 *Offences*

8 (3) A person commits an offence if:

- 9 (a) the person is subject to an order under this section; and
10 (b) the person is capable of complying with a requirement in the
11 order; and
12 (c) the person omits to do an act; and
13 (d) the omission contravenes the requirement.

14 Penalty: Imprisonment for 5 years or 300 penalty units, or both.

15 (4) A person commits an offence if:

- 16 (a) the person is subject to an order under this section; and
17 (b) the person is capable of complying with a requirement in the
18 order; and
19 (c) the person omits to do an act; and
20 (d) the omission contravenes the requirement; and
21 (e) the offence to which the relevant warrant relates is a serious
22 offence.

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

25 **18A Paragraph 201B(1)(a)**

26 After “201(1)”, insert “or 201AA(1)”.

27 **18B Paragraph 201B(1)(d)**

28 After “or (2)”, insert “or 201AA(2) or (4)”.

EXPOSURE DRAFT

Search warrants issued under the Customs Act 1901 **Schedule 4**

1 **18C Paragraph 202(1)(a)**

2 Omit “or 201”, substitute “, 201 or 201AA”.

3 **18D Paragraph 202A(2)(a)**

4 After “201(2)(b)”, insert “or 201AA(4)(a)”.

5 **19 Subsection 203K(5)**

6 After “198(1),”, insert “199A(1),”.

7 **20 Subsection 203M(4)**

8 After “198,”, insert “199A,”.

9 **21 Application of amendments**

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

EXPOSURE DRAFT

Schedule 5 Australian Security Intelligence Organisation

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:

EXPOSURE DRAFT

Australian Security Intelligence Organisation **Schedule 5**

- 1 (a) orally; or
2 (b) in writing.
- 3 (3) If a request under paragraph (1)(a) is made orally, the
4 Director-General must:
5 (a) make a written record of the request; and
6 (b) do so within 48 hours after the request was made.
- 7 (4) The Director-General may enter into a contract, agreement or
8 arrangement with a person or body in relation to conduct engaged
9 in by the person or body in accordance with a request under
10 paragraph (1)(a).
- 11 *Unsolicited disclosure of information etc.*
- 12 (5) If:
13 (a) a person or body engages in conduct that consists of, or is
14 connected with:
15 (i) giving information to the Organisation; or
16 (ii) giving or producing a document to the Organisation; or
17 (iii) making one or more copies of a document and giving
18 those copies to the Organisation; and
19 (b) the person reasonably believes that the conduct is likely to
20 assist the Organisation in the performance of its functions;
21 and
22 (c) the conduct does not involve the person or body committing
23 an offence against a law of the Commonwealth, a State or a
24 Territory; and
25 (d) the conduct does not result in significant loss of, or serious
26 damage to, property; and
27 (e) subsection (1) does not apply to the conduct;
28 the person or body is not subject to any civil liability for, or in
29 relation to, the conduct.
- 30 *Copies of, or extracts from, documents*
- 31 (6) The Organisation may make and retain copies of, or take and retain
32 extracts from, a document given or produced to the Organisation:
33 (a) in accordance with a request under paragraph (1)(a); or
-

EXPOSURE DRAFT

Schedule 5 Australian Security Intelligence Organisation

1 (b) under paragraph (5)(a).

2 *Subsections (1) and (5) have effect despite other laws*

3 (7) Subsections (1) and (5) have effect despite anything in a law of the
4 Commonwealth, a State or a Territory (whether passed or made
5 before or after the commencement of this section) unless the law
6 expressly provides otherwise.

7 *Certificate*

8 (8) The Director-General may give a certificate in writing certifying
9 one or more facts relevant to the question of whether the
10 Director-General was satisfied, on reasonable grounds, that
11 particular conduct was likely to assist the Organisation in the
12 performance of its functions.

13 (9) In any proceedings that involve determining whether subsection (1)
14 or (5) applies to particular conduct, a certificate given under
15 subsection (8) is prima facie evidence of the facts certified.

16 *Compensation for acquisition of property*

17 (10) If the operation of this section would result in an acquisition of
18 property (within the meaning of paragraph 51(xxxi) of the
19 Constitution) from a person otherwise than on just terms (within
20 the meaning of that paragraph), the Commonwealth is liable to pay
21 a reasonable amount of compensation to the person.

22 (11) If the Commonwealth and the person do not agree on the amount
23 of the compensation, the person may institute proceedings in the
24 Federal Court of Australia for the recovery from the
25 Commonwealth of such reasonable amount of compensation as the
26 court determines.

27 **3 At the end of Division 2 of Part III**

28 Add:

EXPOSURE DRAFT

Australian Security Intelligence Organisation **Schedule 5**

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

EXPOSURE DRAFT

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

EXPOSURE DRAFT

Australian Security Intelligence Organisation **Schedule 5**

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

EXPOSURE DRAFT

Schedule 5 Australian Security Intelligence Organisation

1 Penalty for contravention of this subsection: Imprisonment for 5
2 years or 300 penalty units, or both.

172 *Telecommunications and Other Legislation Amendment (Assistance
and Access) Bill 2018* No. , 2018

EXPOSURE DRAFT